دليل الأمان الرقمي

محمد هاني صباغ

أكاديمية حسوب

دليل الأمان الرقمي

تعرف على مفهوم الأمان والخصوصية وكيفية حماية نفسك في العالم الرقمي

تأليف

محمد هاني صباغ

تحرير وإشراف

جميل بيلوني

إخراج فني

مهند مدراتي

عن الناشر

أُنتج هذا الكتاب برعاية شركة حسوب وأكاديمية حسوب.

تهدف أكاديمية حسوب إلى توفير دروس وكتب عالية الجودة في مختلف المجالات وتقدم دورات شاملة لتعلُّم البرمجة بأحدث تقنياتها معتمدةً على التطبيق العملي الذي يؤهل الطالب لدخول سوق العمل بثقة.

حسوب مجموعة تقنية في مهمة لتطوير العالم العربي. تبني حسوب منتجات تركّز على تحسين مستقبل العمل، والتعليم والتواصل. تدير حسوب أكبر منصتي عمل حر في العالم العربي مستقل وخمسات ويعمل فيهما فريق شاب وشغوف من مختلف الدول العربية.

جدول المحتويات

تقديم

مع الغياب التام لأي مصادر مفيدة باللغة العربية عن مجالات الخصوصية والحماية والأمان الرقمي وتأمين الأجهزة الشخصية، جاء هذا الكتاب ليكون شاملًا للكثير من طرق الحماية والأمان التي يحتاج إليها المستخدم العربي المعاصر في مختلف المجالات الرقمية، بل ويتعداها إلى مواضيع متقدمة جدًا في المجال.

إنّ الأمان الرقمي موضوعٌ مهم للحديث عنه وليس شيئًا رفاهيًا أو تكميليًا، خصوصًا مع اطّراد عدد المستخدمين الجدد مع عدد انتهاكات واختراقات الأمان والخصوصية التي تحصل كلّ يوم.

يبدأ الكتاب بعرض المفاهيم الأساسية التي يجب أن يمتلكها أيّ قارئ للكتاب، وهي مفاهيمٌ تعتمد عليها الكثير من الفصول الأخرى في الكتاب فلا غنىً عنها بحالٍ من الأحوال. ثم ينتقل الكتاب إلى الحديث عن الوعي وأهميته، وقد قدّمنا هذا الفصل على غيره لأنّ الوعي مبدأٌ عام يُمكن تطبيقه في مختلف مجالات الحماية الرقمية وليس شرحًا لطريقة تثبيت برنامج أو إضافة مثلًا. كما أنّه أهم طريقة لحماية المُستخدم نفسَه.

ويأتي بعد هذين الفصلين مختلف الفصول التي تشرح اختيار خدماتٍ معينة أو طريقة تأمين أجهزة وأنظمة معينة. يجد القارئ في كلّ فصلٍ من هذه الفصول شرحًا للمفهوم المُراد تأمينه قبل الشروع بطريقة حمايته وتأمينه، وهذا لأنّه يجب أن يسبق العلمُ بالمفهوم العلمَ بحمايته، وإلّا كانت الحماية ناقصة غير مكتملة الأركان.

يفضّل للقارئ المبتدئ أن يقرأ الكتاب كما هو؛ دون محاولة القفز فوق بعض الفصول أو الانتقال إلى غيرها. أمّا بالنسبة إلى القارئ المحترف والمتعمّق في مجال علوم الحاسوب والأمان الرقمي، فيمكنه الانتقال إلى قراءة الفصول التي يريدها من الكتاب فقط إن كان على عُجالة.

تشرح بعض فصول الكتاب مواضيع متقدمة جدًا ونادرة الذكر في الويب العربي، ولذلك

قد يكون فهمها صعبًا في الوهلة الأولى من قراءتها. لكننا ننصح ألّا يتوقف القارئ عندها ويحكم على كامل الكتاب بالصعوبة فيتوقف عنّه، بل أن يكمل القراءة حتّى لو لم يفهمها الآن ويتابع بقية الفصول. وسيجد القارئ أنّه يفهم الفصول السابقة بصورة أفضل كلّما قرأ المزيد منها.

وقد تكون بعض المعلومات شاقّة على الفهم، فننصح القارئ الكريم ألّا يتوقف عندها، ويتابع إلى غيرها. وليعلم القارئ أنّه وإن لم يستفد من هذه المعلومات اليوم فقد يستفيد منها غدًا، فعليه أن يتذكّر أنّه قرأها في هذا الكتاب ليتمكّن من الرجوع إليه.

ومما ركّزنا عليه في كل فصلٍ من الفصول أن نشرح المفهوم الذي نتحدث عنه بِصورة جيدة قبل الشروع في محاولة تأمينه وحمايته، كما قدّمنا الفصول السهلة والبنائية قبل الفصول المتقدمة والصعبة. وهذا لأنّ الكثير من المجالات في الأمان الرقمي متشابكةٌ جدًا مع بعضها البعض؛ حيث تتطلب فهم أكثر من مفهوم سويةً قبل محاولة الشروع في تأمينها.

فلا يُمكن مثلًا تأمين نظام التشغيل دون فهم طريقة عمله، وبرامجه وتحديثاته والاتصالات التي يفتحها والموارد التي يطلبها وعلاقته بالعتاد والكثير من المفاهيم الأخرى السابقة له.

ونشدّد على القارئ الكريم أن يستوعب المفهوم الذي يُتحدّث عنه في تلك الفصول قبل الشروع في عملية الحماية والتطبيق، وهذا لأنّ مجال الأمان الرقمي يرتبط فيه العلم النظري بالعلم التطبيقي بشدّة؛ فلا يكفي أن تطبّق التعليمات دون أن تفهم ما يجري تحت الطاولة بالضبط، وإلّا وقعت في فخّ سوء التدبير وترك ثغراتٍ مكشوفة يمكن لمن يريد أن يتجسس عليك أن يمرّ عبرها.

إنّ هذا الكتاب موجّهٌ بالدرجة الأولى إلى عوام مستخدمي الحواسيب والأجهزة الذكية ويستهدف إفادة معظم المستخدمين، ولا يخلو من مواضيع ومعلومات مفيدة حتّى للخبراء والمتخصصين في المجال. غير أنّ هذا الكتاب ما هو إلّا محاولة لجعل المستخدمين يهتمون بمجال الأمان الرقمي وينتبهون إلى طرق حماية أنفسهم فيه، وليس مرجعًا شاملًا لكلّ شيءٍ في المجال.

أتوجه بجزيل الشكر إلى شركة حسوب لرعايتها مشروع إخراج هذا الكتاب إلى النور، ولم تكتفِ بتلك الرعاية بل أتاحت الكتاب مجانًا لكل من يريد الاستفادة منه عبر أكاديمية حسوب. أنصح القرّاء بالاطلاع على بقية مشاريعها مثل موسوعة حسوب، ومستقل وخمسات.

محمد هاني صباغ

10 شباط 2021

1. لماذا يجب الحفاظ على أماننا الرقمي؟

لعل هذا هو أهم سؤالٍ ينبغي علينا إجابته في بداية هذا الكتاب: «لماذا يجب أن أحافظ على خصوصيتي؟ أنا ليس لدي شيء لأخفيه، ما نوع الضرر الذي يمكن أن يلحق بي أن أعطيتهم بعض معلوماتي»؟ وكلّها أسئلة مشروعة يسألها الناس عندما نخبرهم بوجوب تحرّيهم للأمان والخصوصية عند القيام بأي نشاط رقمي.

هناك جانبان من المهم الفصل بينهما في هذه المسألة:

- الأمان: والمقصود به خلو الخدمات والحواسيب والهواتف التي تستعملها من البرمجيات الخبيثة أو تلك التي تراقب بياناتك بصورة مباشرة وترسلها إلى جهة خارجية أخرى. مثل بعض البرمجيات الخبيثة التي تتجسس على المستخدمين بهدف سرقة أرقام البطاقة الائتمانية أو كلمات المرور، أو رسائل التصيد الاحتيالي التي تهدف إلى اختراق حسابك على فيس بوك مثلًا، أو البرمجيات الضارّة بصورة عامّة والتي تخرّب أجهزتك المختلفة.
- الخصوصية: وهي درجة السرّية التي تتمتع بها أثناء قيامك بالنشاطات المختلفة على الشبكة، وإلى أي حدٍ يمكن للأشخاص الآخرين معرفة مختلف المعلومات عنك إن أرادوا ذلك.

بالنسبة لجانب الأمان، فهو حجر الأساس في مختلف أنشطة المُستخدم الرقمية وهذا لأنّ استخدام أيّ خدماتٍ أو أجهزة مشكوكٍ بأمانها يُعرّضك كمستخدم لاختراق بياناتك وملفّاتك وسرقة معلوماتك وأموالك بصورة قد لا تتخيلها.

فكّر ما إذا حصل أحد المُختَرِقين (Hackers) على وصولٍ إلى هاتفك المحمول مثلًا. بما أنّ صورك وكلمات المرور لمواقع الويب المُختلفة التي تستعملها محفوظةٌ عليه فقد صارت كلّها بيده الآن، ويُمكنه استخدامها كيفما شاء أو ابتزازك بها وهذه مصيبة. وقد يسرق معلومات بطاقتك

الائتمانية ويسحب منها أموالًا دون أن تدري. ويظنّ الكثير من الناس أنّ تأمين هواتفهم المحمولة عملية تافهة لا تحتاج كلّ هذا الكلام أو قراءة كتب أو ما شابه، ولكن ما يغفلون عنه هو أنّ هذه العملية صعبة وتحتاج دراسةً في الواقع وليست كما يظنون.

اكتُشفت مثلًا ثغرة في أنظمة أندرويد للهواتف المحمولة سنة 2019م [1] تصيب أكثر من مليار جهاز - جهازك غالبًا منها - تسمح للمُختَرقين بتحويل كامل تدفّق الشبكة (Network Traffic) الخاصّ بالجهاز إليهم وبالتالي اختراق كل نشاطاتك وبياناتك على الشبكة عبر مجرّد رسالة نصية (SMS) يُرسلونها إلى أيّ هاتف يريدونه. اكتُشفت كذلك ثغرة أمنية قبل 5 أشهر فقط من تاريخ هذا الكتاب في نظام iOS لمختلف الأجهزة المحمولة من شركة آبل [2]، في تطبيق البريد الخاصّ به حيث أنّه بمجرّد تحميل ملفّ خبيث (دون تشغيله حتّى!) يُصبح للمخترقين وصولٌ شبه كامل لكل شيء موجود على الجهاز.

يجهل الكثير من الناس في حالة هواتف أندرويد مثلًا أنّ هواتفهم لا تتلقى أيّ تحديثات بعد أوّل سنة من إطلاقها من طرف الشركة المصنّعة، وبالتالي كلّ الثغرات الأمنية التي تُكتشف على مدار السنين اللاحقة لا تصل ترقيعاتها وإصلاحاتها إلى المستخدمين بتاتًا، وهو ما يعني أنّ الأجهزة المحمولة للملايين من المستخدمين عرضة للاختراق بشربة ماء.

الحواسيب ليست أفضل؛ اكتُشفت ثغرة أمنية في تطبيق مايكروسوفت أوفيس سنة 2017م تسمح للمُخترقِين بالتحكّم بكامل الحاسوب عبر إرسال ملفّات مستندات تحتوي على برمجياتٍ خبيثة. الآن قد يظنّ أحدهم أنّ الثغرة انتهى وضعها بما أنّها قد اكتُشفت قبل 3 سنوات وأُصلحت، لكن هذا ليس صحيحًا للأسف فالثغرة هي واحدة من أكثر 10 ثغرات أمنية استخدامًا من قِبَل المُختَرقِين على الإطلاق إلى 2020م! [3] وهو ما يعني أنّ المستخدمين لا يقومون بتحديث أنظمتهم بالشكل الكافي لتحصينهم من هذه الثغرات.

ويستخدم الكثير من الناس البرامج والأنظمة مكسورةَ الحماية (Cracked Software) ظانين أنه لا يوجد بها مشكلة تمنع من استعمالها. ولا يدركون أنّ هذه البرامج مكسورة الحماية من طرف هؤلاء المُخترقِين أصلًا وهم من يديرون الكثير من مواقع الإنترنت والمدوّنات لنشر روابط هذه البرمجيات المكسورة، وهذا لأنّهم يكونون قد شحنوا فيها أطنانًا من برمجيات التجسس والفيروسات بالفعل وكلّ ما يريدونه هو التسويق لها، فيأتي المستخدمون ويبتلعون الطعم كالسمكة.

يُستعمل هذا النمط بشدّة في هجمات برامج الفِدية (Ransomware)، وهي برمجيات تقوم بتشفير كامل القرص الصلب ونظام التشغيل وتمنع المستخدم من الوصول إليها وفكّ تشفيرها إلّا بعد أن يقوم بتحويل مبلغٍ طائل من المال إلى المُخترقِين ليرجعوا له بياناته. فيقوم المخترقون

بوضع هذه البرمجيات داخل الأنظمة مكسورة الحماية وينشرونها للمستخدمين، ولا يفعّلون تلك الثغرات مباشرةً بل ينتظرون استخدام عددٍ كبير من المستخدمين لها قبل أن يقوموا بذلك. وقد يقومون بنشرها عبر طرقٍ مختلفة وليس فقط برمجيات كسر الحماية (Crack).

أشارت الإحصائيات إلى أنّ ربع شركات بريطانيا مثلًا سنة 2018م قد أصابتها فيروسات الفدية هذه [4]، وقد أصاب فيروس الفدية الشهير WannaCry ملايين الأجهزة حول العالم مخلّفًا مليارات الدولارات من الخسائر سنة 2017م [5] بسبب ثغراتٍ أمنية في نظام ويندوز.

يُصبح موضوع الأمان الرقمي أكثر أهميّة مع تزايد الأجهزة الذكية المحيطة بنا فكلّ هذه الأجهزة هي نقاط هجوم للمُخترقِين، ويمكنهم التجسس عليك وسماع أصواتك أو رؤيتك عبر الكاميرات التي بها دون أن تشعر أنت بذلك كمستخدم. ويجهل الكثير من الناس أنّ المُخترقِين قد يكونون نجحوا بالفعل في اختراق أجهزته ولكنّهم لا يصدرون أيّ حركة مشبوهة تجنّبًا لشعور المُستخدم بذلك، فيكتفون بالتجسس على نشاطاتك ومراقبة مواقع الويب التي تزورها ورفع صورك وملفّاتك إليهم دون محاولة سرقة بطاقاتك الائتمانية مثلًا أو اختراق حساباتك على مواقع التواصل، فهذه النشاطات الأخيرة ستنبّه المستخدمين مباشرةً إلى وجود أحدهم يتجسس عليهم، وبالتالي يكتفون بجمع البيانات دونًا عن التدمير المباشر.

وتزداد أهميّته عندما يكون للفرد عائلة؛ لا تفكّر فقط بأجهزتك أنت بل فكّر بأجهزة أخواتك أو أولادك أو والدك أو والدتك، هؤلاء غالبًا ما يكونون أقل قدرةً على معرفة ما يجري من الأمور التقنية وراء هذه الأجهزة وبالتالي هم أكثر عرضة للاختراق وسرقة بياناتهم وملفّاتهم وصورهم. ويصبح الموضوع فاجعة كبيرة إن حصل هذا.

كلّ ما سبق هو ما يتعلّق بجانب الأمان الرقمي، أمّا في موضوع الخصوصية، فهي مهمّة جدًا كذلك خصوصًا في أوقاتنا الراهنة. هل حقًا لا مشكلة لديك في أن يعرف كل طلاب الجامعة التي تدرس فيها أو مكان العمل الذي تعمل فيه مثلًا معلوماتك الشخصية ومعلومات أسرتك وعائلتك، وصوركم وملفّاتكم وأين تعملون ومع من ومنذ متى وكيف؟

الموضوع أشبه بشخص قادم من الشارع ليقول لك: «أعطني بعضًا من صورك وملفاتك ومعلوماتك» ثم تقوم أنت طواعية - للأسف الشديد - بإعطائها له. وهذا ما يقوم به معظم الناس للأسف حيث ينشرون طواعيةً كلّ صورهم ونشاطاتهم على مواقع التواصل لمن هبّ ودبّ، ويمكن استعراض كلّ المعلومات المتوفّرة عنك على الشبكة عبر كتابة اسمك في جوجل أو فيس بوك، ببساطة.

قد تُستخدم البيانات بطرقٍ مُختلفة بناءً على من يجمعها ولماذا؛ فيُمكن بسهولة لأجهزة الاستخبارات الأجنبية معرفتك ومراقبة تحرّكاتك عبرها، ويُمكن للمُتنمرّين على الإنترنت (الأشخاص المجهولون الذين لا همّ لهم سوى تدمير حياة الآخرين فقط للتسلية) استخدامها ضدك ومُراسلة معارفك بمعلومات مزيّفة لتشويه سمعتك، ويُمكن للشبكات الإعلانية ومراكز البيع أن تستخدمها لتحاول بيعك منتجًا لا تريده ولا تحتاج إليه ومع ذلك تنجح في بيعك إيّاه لأنها تعرف شيئًا من بعض جوانبك النفسية. كما يُمكن للكثير من الجهات الأخرى أن تستخدم حتّى أتفه المعلومات ضدك بطرقٍ لا يمكن لك حتّى أن تتخيلها.

عند قيامك بعمل مقابلة عمل مثلًا فأوّل ما قد يُطلب منك قبلها هو حساباتك على مواقع التواصل. تُشير الإحصائيات [6] إلى أنّ 70% من كلّ مُدراء التوظيف حول العالم يتحققون من حسابات الموظفين المحتملين قبل القيام بتوظيفهم، و45% منهم يتحققون من حسابات الموظفين العاملين لديهم بالفعل. لِذا فكل ما تنشره عن نفسك من معلوماتك بما في ذلك آراؤك السياسية والاجتماعية والدينية قد يُستعمل ضدك ويضرّك في مراحل لاحقة من حياتك. ويكفي فقط كتابة اسمك الحقيقي على جوجل أو فيس بوك لرؤية تلك المعلومات.

وكم من المشاكل الاجتماعية والأسرية التي حصلت بسبب غياب عامل الخصوصية هذا، حيث ينشر الناس كلّ شيءٍ عنهم فيأتي الآخرون ويستخدمون هذه المعلومات ضدّهم.

ولا يحسب الكثير من المستخدمين أهمية هذه البيانات في المستقبل للأسف، بل يقيسون الأمر على الحاضر فقط. ربّما ليس لديك شيءٌ لتخفيه اليوم لكن هل لن يكون لديك مشكلة إذا قام أحدهم باستعراض سجل صورك ومشاركاتك المختلفة على المنتديات والمعلومات الأخرى التي نشرتها عن نفسك قبل 5 سنوات، ثم جاء لينشرها اليوم بعد أن صرت ربما سياسيًا مشهورًا أو أستاذًا جامعيًا أو شخصًا مهمًا في المجتمع؟ كيف يمكنك أن تضمن أنّ ذلك لن يكون مهمًا لك في المستقبل؟

1.1. ختام الفصل

من المهم أن تحاول الحفاظ على خصوصيتك وأمانك على الشبكة بأقصى درجة ممكن لكل الأسباب السابق ذكرها. وموضوع هذا الكتاب ليس شيئًا هامشيًا أو رفاهيًا لا يحتاج إليه أحد بل هو موضوعٌ حسّاس على الجميع الاهتمام به وزيادة وعيهم حوله.

وكم من مشاكل اجتماعية وحالات طلاق وحالات اختراق وسرقة وحالات اعتقال وتعذيب وقتل حصلت بسبب غياب عامليّ الأمان والخصوصية على الشبكة. لا تنسَ ذلك وأنت تقرأ فصول هذا الكتاب!

2. مفاهيم تأسيسية عن الأمان الرقمي

سيحوي هذا الفصل مجموعةً من المفاهيم والتعريفات التي تحتاج إليها لفهم عمل الأشياء الأساسية من حولك. من الضروري أن تفهم طريقة عمل هذه الأشياء لتفهم قدرات الآخرين على تعقّبك وسرقة بياناتك بالإضافة إلى كيفية تأمين نفسك ضدها.

هذه التعريفات ما هي إلّا رؤوس أقلام وتعريفات سريعة للأشياء المذكورة، فبالنهاية يهدف هذا الكتاب إلى شرح طُرق تأمين خصوصيتك وأمانك الرقمي، وليس تعليمك علوم الحاسوب ككل. إن أردت الاستزادة حول هذه المواضيع فيُمكنك البحث عنها في ويكيبيديا أو مشاهدة الفيديوهات المختلفة على يوتيوب.

2. 1. الحاسوب والهاتف الذكي ونظام التشغيل

الحاسوب هو جهازٌ مكوّن من قسمين: البرمجيات (Software) والعتاد (Hardware)، وبدمج هذين القسمين يمكننا الحصول على آلة يمكننا تشغيلها للقيام بالآلاف من المهام التي نحتاج إليها في حياتنا اليومية.

يتكونّ عتاد الحاسوب من مُعالج (CPU) وهو الوحدة التي تقوم بالعمليات الحسابية المعقّدة في الحاسوب وتعتبر كعقل الجهاز، بالإضافة إلى الذاكرة العشوائية (RAM) التي تقوم بتخزين العمليات والبرامج ونظام التشغيل الذين يعملون حاليًا، والقرص الصلب (Hard disk) الذي يعمل كوسيط لتخزين الملفّات والمجلّدات على المدى البعيد، وبطاقة الرسوميات (Graphics Card) المسؤولة عن عرض الرسوم والألوان والصور على الشاشة، واللوحة الأمّ (Motherboard) التي تقوم بربط كل هذه القطع والمئات من القطع الصغيرة الأخرى ببعضها البعض.

عندما تضغط على زرّ تشغيل الحاسوب، ما يحصل هو أنّه أولًا يتم تحميل ما يُعرف بالبيوس BIOS من ذاكرة ROM (وهي ذاكرة أخرى موجودة في الحاسوب، لكن على عكس الذاكرة من نوع RAM-، فإنّه لا يتم مسح جميع محتوياتها عقب عمليات إيقاف التشغيل وإعادة التشغيل، بل تحتفظ بمحتوياتها بصورة دائمة، وهي وحدة تخزين صغيرة جدًا تحتوي فقط على النظام الإقلاعي الأساسي الخاص بالحاسوب والمسمّى BIOS)، ثم يحمِّل نظام البيوس BIOS الأساسي نظام التشغيل أو أجزاء منه إلى الذاكرة العشوائية من القرص الصلب، ثم يتم تشغيل وتنفيذ الشفرة البرمجية (Code) الخاصّة بنظام التشغيل عبر المُعالج، وهو ما يسمح بتشغيل بقية قطع العتاد الأخرى. ثم بعد أن تتم عملية إقلاع نظام التشغيل عبر محمل الإقلاع (Bootloader)، يُعرَض سطح المكتب أو الشاشة الرسومية لك عبر بطاقة الرسوميات وتصبح قادرًا على تشغيل البرامج والتطبيقات العادية لأداء مهامك كتصفّح الإنترنت أو كتابة المستندات أو تشغيل الألعاب.

أمّا من طرف البرمجيات (Software)، فأوّل قطعة برمجيات يتعامل معها الحاسوب بعد الإقلاع هي نواة نظام التشغيل، حيث يحمِّلها إلى الذاكرة العشوائية. بعدها يُحمَّل نظام مدير الإقلاع الخاص بنظام التشغيل (systemd مثلًا على أنظمة لينكس)، وهو البرنامج المسؤول عن تحميل بقية البرامج الإقلاعية اللازمة الأخرى وصولًا إلى سطح المكتب النهائي. هناك تفاصيل كثيرة أخرى قبل وأثناء وبعد هذه الخطوات، لكن هذا هو السير العام لطريقة عمل الحاسوب.

الهاتف الذكي لا يختلف كثيرًا عن عن الحاسوب، الفرق الأساسي هو أنّ الهاتف أصغر بكثير ومربوط غالبًا بشاشة لمس، كما أنّ موارد وقدرات الحواسيب العادية أكبر بكثير من الهواتف الذكية العادية.

هناك 3 عوائل أساسية لأنظمة تشغيل الحواسيب: ويندوز وماك ولينكس، معظم الحواسيب المكتبية حول العالم تستخدم نظام التشغيل ويندوز القادم من شركة مايكروسوفت، بينما يتقاسم ماك ولينكس بقية الحصّة. يمكنك استبدال وتثبيت أي نظام تشغيل تريده على حاسوبك متى ما شئت.

أمّا بالنسبة للهواتف الذكية، فهناك نظامان شهيران للتشغيل هما أندرويد (تطوره شركة جوجل) وiOS (تطوره شركة آبل). لكن هنا، على عكس ما يحصل في الحواسيب، فإنّ الهواتف الذكية غالبًا ما يكون عليها قيود أكبر فيما يخصّ نظام التشغيل؛ فتجد أنّه لا يمكنك استبدال نظام التشغيل أو تغييره في الكثير من الأحيان، وحتّى عندما يكون بإمكانك فعل ذلك، فإنّ العملية معقّدة وطويلة وتستغرق الكثير من الوقت، وستتسبب حتمًا بفقدانك للضمان المُرفق مع الجهاز (شركات تصنيع الهواتف الذكية جميعها تقريبًا تقول لك: «إذا غيَّرت نظام التشغيل أو تلاعبت فيه فإننا نتخلى تمامًا

عـن صيانـة جهـازك لـو تعطّـل، حتـى لـو كان العطـل متعلقًـا بالعتـاد وليـس البرمجيـات»)، كمـا أنّـه فـي الغالـب تتحكّـم الشـركة المطـوّرة لنظـام التشـغيل بالنظـام الموجـود علـى جهـازك بصـورة مركزيـة كبيـرة وتقـرر هـي أن تمـدّك بالتحديثـات أو ألّا تمـدك بهـا موازنـةً بأنظمـة سـطح المكتـب.

جميـع الهواتـف الذكيّـة تحـوي علـى نُسـخٍ معدّلـة مـن أنظمـة التشـغيل هـذه لتتوافـق مـع عتـاد الهاتـف القـادم مـن الشـركة المصنّعـة للعتـاد، وهـي عمليـة كبيـرة تتـم بيـن الشـركات المصنّعـة للهواتـف وبيـن الشـركات المطـوّرة للأنظمـة بصـورة مباشـرة.

2. 2. البرامج والتطبيقات

فـي البدايـة دعنـا نتعـرّف علـى مُصطلـح «الشـفرة البرمجيـة» (Code) بصـورة أفضـل. الشـفرة البرمجيـة هـي نصـوص يكتبهـا المبرمجـون والمطـورون لجعـل الحواسـيب والهواتـف الذكيـة تفهـم مـا يريـده المطـورون أن تفعلـه، فالحواسـيب لا تفهـم اللغـات المحكيّـة العاديـة بـل تتعامـل مـع رقميّ الصفـر والواحـد فقـط (01010101 مثـلًا). فـإذا أراد المبرمـج مثـلًا كتابـة نظـام تشـغيل للحاسـوب، فإنّـه يكتـب أولًا الشـفرة البرمجيـة لنظـام التشـغيل، ثـم يتـم ترجمـة تلـك الشـفرة البرمجيـة التـي يكتبهـا إلـى الأرقـام الثنائيـة (0 و1) مـن طـرف برنامـج وسـيط يعـرف بالمُصـرّف (Compiler) يعمـل كحلقـة الوصـل بيـن المبرمـج والحاسـوب، ثـم تنفّـذ تلـك الأرقـام مـن طـرف المُعالـج ليقـوم الحاسـوب بعدهـا بفهـم مـا يريـده المبرمـج والقيـام بـه.

البرامـج هـي شـفرات برمجيـة مُهندسـة ومنظّمـة بطريقـة معيّنـة لأداء مهـام معيّنـة قـد يحتـاج إليهـا المسـتخدم. هنـاك ملاييـن الأشـخاص والشـركات والمؤسسـات حـول العالـم الذيـن يقومـون بكتابـة برامـج مختلفـة لأداء مهـام مختلفـة يحتـاج إليهـا النـاس عبـر الحواسـيب أو الهواتـف الذكيـة.

قـد تكـون البرامـج مفتوحـة المصـدر (Open Source) وقـد تكـون مغلقـة المصـدر (Closed Source) وهنـاك أنـواعٌ أخـرى غيرهمـا (مثـل Freeware).

تسـمح لـك البرامـج المفتوحـة المصـدر برؤيـة شـفرتها المصدريـة وتعديلهـا وتوزيعهـا ونسـخها بصـورة حـرّة تمامًـا (حسـب شـروط الرخصـة)، بينمـا البرمجيـات المغلقـة المصـدر لا تسـمح لـك بذلـك، بـل تتطلـب منـك الحصـول علـى «اتفاقيـة رخصـة المُسـتخدم النهائـي» تُعـرف بـ «EULA» (وهـي اختصـار لـ End-User License Agreement)، تسـمح لـك باسـتخدام البرنامـج علـى جهـاز واحـد فقـط ولا تسـمح لـك بنسـخه ولا توزيعـه ولا تعديلـه ولا رؤيـة شـفرته البرمجيـة. مـن بيـن أشـهر تراخيـص البرمجيـات المفتوحـة: GPL, MIT, Apache, AGPL, BSD.

بعض البرامج قد تكون مدفوعة وبعضها قد يكون مجانيًا، وبعضها قد يأتي مع الشفرة البرمجية الخاصة به وبعضها قد لا يأتي معها. معظم البرمجيات في العالم احتكارية (مغلقة المصدر ومدفوعة).

2. 3. البرامج الخبيثة والثغرات الأمنية

البرامج الخبيثة (كالفيروسات مثلًا) تتسلل إلى جهازك بطرقٍ شتّى وتقوم إمّا بتخريبه أو سرقة بياناتك ومعلوماتك الحساسة ككلمات المرور والبطاقات الائتمانية، أو تقوم باستخدام ملفّاتك رهينةً إلى أن تقوم بدفع مبلغٍ معين من المال لقاء إلغاء قفله (وهي تدعى بفيروسات الفدية Ransomware). هناك أنواعٌ كثيرة أخرى من البرامج الخبيثة، مثل الديدان (Worms) وأحصنة طروادة (Trojan Horse)، وتمتلك مسمّيات مختلفة كما ترى بسبب اختلاف طريقة عملها وأدائها للتخريب على أنظمة المستخدمين. هناك العشرات منها وهي أكثر من أن تحصى.

يمكن للفيروسات أن تنتقل عبر طرقٍ شتّى؛ إمّا عن طريق زيارة مواقع مشبوهة عبر الإنترنت، أو تحميل تطبيقات ملوّثة بالفيروسات من الإنترنت، أو عبر فلاشات الـUSB، أو عبر الملفّات المرفقة بالبريد الإلكتروني ... إلخ. هناك الكثير من الطرق الأخرى.

الثغرات الأمنية (Security Vulnerabilities) هي ضعف بالبرامج أو نظام التشغيل الذي تستخدمه، مما يسمح للمُخترقِين باستغلال نقطة الضعف هذه من أجل اختراقك وسرقة بياناتك. تكون الثغرات الأمنية ناتجة عن خطأ المبرمجين والمطورين في أسلوبهم في البرمجة في الكثير من الأحيان، فيقومون بكتابة شفرة برمجية سيئة مما يجعل النظام أو البرنامج عرضةً لسرقة البيانات والملفّات عبر شنّ هجوم على جهازك. لكن الثغرات الأمنية ليست محصورة على المبتدئين في البرمجة فقط، بل حتّى أفخم الشركات البرمجية وأكثرها تخصصًا قد تعاني منها حيث تكون الثغرة الأمنية مخفية بطريقة يكون من الصعب جدًا الانتباه لها، فالثغرات البرمجية ستظل دومًا موجودة، لأنّه لا يمكن لبشر أن يصنع الكمال.

يُشتبه ببعض الشركات البرمجية العملاقة، وخصوصًا مايكروسوفت [2]، أنّها تترك الكثير من الثغرات الأمنية في منتجاتها عن قصد بهدف مساعدة أجهزة الاستخبارات الغربية على اختراق أجهزة المستخدمين دون أن يعلموا بذلك. لم يُكشف حتّى اليوم عن بروتوكول تعاون شبيه بهذا، لكن عدد الثغرات الهائل المُكتشف في منتجات مايكروسوفت المُختلفة مثل متصفحها إنترنت إكسبلورر، ونظام التشغيل ويندوز وتطبيقات مايكروسوفت أوفيس المكتبية يضعنا موضعًا للشكّ

لمثل هكذا احتمال. فالمقصود عمومًا هو أنّ الثغرات الأمنية قد لا تكون دومًا عن طريق الخطأ، بل قد تكون متعمّدة.

2. 4. الأذونات (Permissions)

تمتلك معظم أنظمة التشغيل أنظمة «أذونات» خاصّة بها لتقييد إمكانيات البرامج العاملة عليها ووصولها إلى مختلف أجزاء نظام التشغيل. فقد يمنع نظام التشغيل بعض البرامج من الوصول إلى مجلّدات معيّنة في النظام تجنّبًا للعبث بها أو تخريبها، كما قد يمنع وصول البرامج إلى بعض أجهزة العتاد مثل المجهار (الميكرفون) والكاميرا دون إذنٍ مسبق من المستخدم، وغير ذلك من التقييدات.

مبدأ الأذونات مهم جدًا - خصوصًا على الهواتف المحمولة - وهذا لأنّه خطّ الدفاع الأوّل من التطبيقات المشبوهة التي قد يحمّلها المستخدم دون أن يدري أنّها تخرّب نظامه، ولهذا فإنّ قيام نظام التشغيل بتقييدها افتراضيًا يحلّ تلك المشكلة ويقلل من ضررها.

تمتلك مختلف أنظمة التشغيل طرقًا مختلفة للتعامل مع الأذونات وما المسموح به وما الممنوع.

2. 5. التحديثات

بسبب ما سبق، يقوم المبرمجون والمطورون بإرسال تحديثات إلى المستخدم لإصلاح الثغرات الأمنية أو أي مشاكل أخرى في البرامج أو إضافة مزايا جديدة. قد تختلف طريقة حصولك على التحديث بناءً على نظام التشغيل والبرنامج الذي تستخدمه، فبعض البرامج مثل متصفّح فيرفكس على نظام ويندوز يمتلك ميّزة التحديث التلقائي، مما يضمن تحديثه أولًا بأول، بينما على لينكس مثلًا، يجب عليك تحديث فيرفكس يدويًا من مدير الحزم (أو تفعيل التحديث التلقائي بصورةٍ ما من طرف النظام).

يُنصح دومًا بالتحديث للإصدارات الجديدة أولًا بأول. لكن في بعض الأنظمة الحساسة وأنظمة الشركات والمؤسسات، التحديث عملية معقّدة جدًا؛ لأن بعض التحديثات قد تقوم بإزالة بعض المميزات أو تعطيل بعض المهام للشركات والمؤسسات، لذلك تمرّ التحديثات في هذه الشركات والمؤسسات بعملية طويلة جدًا من التحقق من الجودة (Quality Assurance) والاختبار لضمن أنّ هذه التحديثات لن تحطّم أي احتياجٍ من احتياجات المؤسسة عند تطبيقها.

لكن بالنسبة لك كمستخدم عادي فحاول البقاء على تحديث برمجياتك أولًا بأول. وإن لم تحدّث نظامك وبرامجك بصورة مستمرة فقد يصبح أكثر عرضة للإصابة بالثغرات الأمنية والبرمجيات الخبيثة.

2. 6. النسخ الاحتياطي

النسخ الاحتياطي (Backup) ببساطة هي عملية نسخ الملفّات إلى وسيطٍ خارجي لحمايتها من الفقدان في حال تعرّضت النسخة الأصلية إلى التلف لأيّ سببٍ من الأسباب. فيمكنك مثلًا نسخ صورك وملفّاتك المهمّة من هاتفك المحمول إلى مكانٍ آخر (خدمة مزامنة سحابية مثلًا) لتتمكن من استرجاعها لاحقًا حتّى لو فقدت هاتفك المحمول لأيّ سببٍ من الأسباب.

يمكن للجميع نسخ ملفّاتهم احتياطيًا عبر تجميعها في مجلّد (أو عدّة مجلّدات) ثمّ ضغطها ورفعها إلى وسيطٍ آمنٍ يثقون به. وفي حال حصل مكروهٌ للنسخة الأصلية من بياناتهم فيمكنهم استرجاع النسخة المحفوظة بسهولة عبر تحميلها من جديد.

هناك طرقٌ وأساليب مختلفة للقيام بعمليات النسخ الاحتياطي وهي تختلف بحسب الاحتياجات والحجم؛ فالشركات العملاقة مثل فيس بوك مثلًا لديها ما يُعرف بعمليات النسخ في الوقت الحقيقي (Real-time Backups) بالإضافة إلى أنظمة نسخ احتياطي معقّدة تجنّبًا لفقدان بيانات أيّ مستخدم، وهي تختلف كلّيًا عن أنظمة النسخ الاحتياطي للمستخدمين العاديين مثلًا.

2. 7. التشفير

التشفير (Encryption) هو عملية تحويل البيانات الصرفة (Plaintext) إلى رموز غير قابلة للقراءة والفهم بهدف حمايتها من المتطفّلين، وهو علمٌ كبير وتقوم عليه كل الأنشطة المتعلّقة بالمال والاقتصاد أو أي شيء متعلّق بالأمان عمومًا على الإنترنت. هناك خوارزميات مختلفة لتشفير البيانات ولكل واحدة منها مميزات وعيوب.

فلنفرض أنّه لديك رقم مثل «779900»، إذا كنتَ تريد تشفيره وفق خوارزمية MD5 (أحد خوارزميات التشفير الشهيرة)، فستحصل على هذا النص:

```
284692BA1391AF100984722BD1FFADD0
```

هذا يعني أنّه لا يمكن لأحدٍ سواك أنت معرفة النص الأصلي، لأنّ النص المشفّر غير قابل للقراءة والفهم وهو مولَّد عن طريق خوارزميات معقدّة لا يمكن كسرها أو فكّ شفرتها. لذلك فإذا

أراد أحدهم إرجاع النص المشفَّر السابق إلى 779900، فيجب عليه أن يجلس ويخمّن الرقم أو النص الذي يُطابق تلك الشفرة، وهي عملية صعبة قد تستغرق أيام أو سنوات بناءً على تعقيد النص الأصلي الغير مشفّر بالإضافة إلى القدرة الحسابية للجهاز الذي يستخدمه من يحُاول كسر التشفير. تُعرف هذه الطريقة بالقوّة الغاشمة (Bruteforce).

لا يُستخدَم التشفير بهذه الطريقة بكثرة، بل يُشفّر ملفّ كامل من البيانات مثلًا أو رسالة بريدية إلكترونية، ثم يُنشَئ ما يعرف بالمفتاح (Key)، وهو ببساطة كلمة سرّ يمكنك أن تعطيها للأشخاص الذين تريدهم أن يتمكّنوا من استخراج البيانات المشفّرة. سيستخدم أولئك الأشخاص المفتاح الذي أعطيتهم إياه لفكّ تشفير البيانات والحصول على محتواها الأصلي، ولا يمكن سوى لك أنت وللجهات التي تريدها أن تطّلعوا على محتوى البيانات، أمّا أي جهة غير مخوّلة بذلك فلن تتمكن من اكتشاف البيانات الأصلية.

وهذا هو أساس بروتوكول HTTPS الذي ستراه لاحقًا، فما يحصل هناك هو أنّ البيانات التي يتم تداولها بين جهازك وبين مواقع الإنترنت يتم تشفيرها منذ أول لحظة اتصال بينك وبينهم، ثم عندما تزور مواقع الإنترنت التي تعمل ببروتوكول HTTPS، تقوم هذه المواقع بإبراز شهادة الاستيثاق (Certificate) والتي تحتوي مفتاح كسر التشفير. وبعدما يستلم متصفّحك المفتاح سيصبح قادرًا على عرض البيانات لك. هناك شركات تقوم بتوزيع هذه الشهادات، وهذه الشهادات يكون منها نسخة مضمّنة في متصفّحات الويب نفسها، فعندما يقوم موقع الويب بإبراز الشهادة الصحيحة التي تبيّن أنّه يتبع التشفير الصحيح، يتم مطابقة تلك الشهادة مع الشهادة الموجودة محليًا للتحقق منها، وبعد نجاح العملية، يتم تسليم المفتاح.

التشفير هو أنجح الطرق لحماية البيانات، وحتّى أعتى وكالات التجسس والاختراق في العالم لا تمتلك بعد القدرة اللازمة على كسره وتحطيمه، بالطبع، بعض الخوارزميات السيئة مثل SHA-1 وMD5 من السهل كسرها عن طريق هجمات القوة الغاشمة (Bruteforce)، لكن الخوارزميات الأقوى مثل SHA-256 وSHA-512 يكون تخمينها لكلمات المرور المعقّدة مستحيلًا على أرض الواقع. لذلك ننصحك دومًا بتشفير بياناتك وملفّاتك وكل شيء مهم.

هناك أنواع وطرق مختلفة للقيام بالتشفير، لكن من بينها ما يُعرف بـ«تشفير طرف لطرف» (End-to-End Encryption) وهو تشفيرٌ يعني ببساطة أنّه فقط المستقبل والمُرسل قادران على إلغاء تشفير الاتصال بينهما دونًا عن أيّ جهة خارجية، بما في ذلك الشركة المزوّدة للخدمة نفسها. لهذا فإنّ الخدمات التي تستعمل هذا النوع من التشفير آمنة جدًا على عكس غيرها.

ننصحك بقراءة كتاب «التشفير، مقدّمة قصيرة جدًا» للمزيد من المعلومات عن التشفير.

2. 8. مفهوم الشبكات والإنترنت والاتصال بهما

التعريف الرسمي للإنترنت هو أنّه عبارة عن «شبكة مكوّنة من مجموعة شبكات»، فما هي الشبكة (Network)؟ ببساطة هي عددٌ من الأجهزة المرتبطة ببعضها البعض. ترتبط هذه الأجهزة ببعضها عن طريق أسلاك (Cables) أو دون أسلاك عن طريق أجهزة الاتصال اللاسلكية (Wireless)، ويكون في كل هذه الأجهزة جهاز صغير هو بطاقة الشبكة (Network Adapter) ليسمح لها بإنشاء الاتصال بين بعضها البعض. الإنترنت ما هو إلّا مجموعة كبيرة من هذه الحواسيب التي تكون متصلة على مدار الساعة وفقًا لآليات وبروتوكولات معيّنة.

لا نريد الخوض للكثير من التفاصيل في هذا الكتاب، لكن لتفهم طريقة عمل الإنترنت بسرعة فافهم الشرح الآتي:

لدى كل جهاز حاسوب أو هاتف محمول ما يُعرف بعنوان الآي بي (IP Address)، وهو عبارة عن رقم يمثّل تمامًا عنوان المنأحزل الخاص بكل شخصٍ منّا، إذ يسمح للأشخاص بأن يعثروا علينا وعلى مكاننا الجغرافي وأن يتمكّنوا من التواصل معنا.

عندما تكتب اسم نطاق موقع معيّن مثل (Google.com) داخل مربّع البحث في متصفّحك، فما يحصل هو أنّ متصفّحك سيُرسل طلبًا (Request) إلى نظام تحديد أسماء النطاقات (Domain Name System) ليطلب منه البحث عن عنوان الآي بي (IP Address) الخاص بموقع Google.com، فيقوم نظام الـDNS بالبحث عن اسم النطاق Google.com في جدولٍ ضخم مخزّنٍ لديه ويكتشف إلى أي عنوان آي بي يعود، ثم يقوم بإرجاع ذاك العنوان لمتصفّحك.

هذه العملية الطويلة تحصل لأنّ الناس يريدون كتابة نصوص مثل Google.com, Youtube.com, Gmail.com وغيرها لفتح مواقع الويب، ولا يريدون كتابة عناوين الآي بي الطويل وتذكّرها (مثل 211.3.138.12)، ببساطة لأنّه لا يمكنهم تذكّر كل تلك العناوين الطويلة الصعبة لكل مواقع الويب التي يزورونها وبالوقت نفسه لا يمكن للحواسيب والآلات أن تفهم وتتعامل سوى بالأرقام، لذلك برزت الحاجة لاستخدام نظام الـDNS.

كما قلنا سابقًا: عنوان الآي بي ما هو إلّا عنوان لجهاز، وأنت عندما تريد فتح موقع Google.com، فإنّ متصفحك يرسل طلبًا إلى ما يُعرف بالخادوم (Server) الذي يعمل وراء الموقع ليقوم بمعالجة طلبك وإرجاع صفحات الويب والرسوم التفاعلية والمحتوى وكل شيء آخر تريده من موقع Google.com. الخادوم هو حاسوب ذو إمكانيات قوية لمعالجة الطلبات التي تأتيه من كافّة أنحاء العالم، وهو الذي يقوم على تلبية طلبات الزائرين والمستخدمين.

متصفّحك يقول للخادوم الذي يعمل على عنوان 216.3.128.12 أنّك تريد تصفّح الموقع، وتطلب منه أن يسمح لك بذلك وأن يقوم بفتح اتصالٍ معك لكي يفتح لك الموقع. بعد أن يفتح الاتصال، يمكن لمتصفّحك وللخادوم أن يتبادلا البيانات من طرفٍ لآخر بهدف خدمتك بالشكل المطلوب.

2. 9. عنوان الآي بي (IP Address)

كما قلنا سابقًا فإن عنوان الآي بي هو عبارة عن عنوان لمعرفة طريقة الوصول إلى الجهاز أو الخادوم المطلوب. يمكن أن تشترك الكثير من الأجهزة على عنوان آي بي واحد، لكن عمومًا، لا يمكن لجهاز سواء كان حاسوبًا عاديًا أو خادومًا أن يمتلك أكثر من عنوان آي بي (ولكن هناك استثناءات).

لذلك، وبينما تتصفّح الإنترنت، يُمكن للمواقع التي تزورها، ومزوّد الإنترنت الذي تستخدمه، والدولة التي أنت تعيش بها، ونظام تحديد أسماء النطاقات الذي تستخدمه أن يعرفوا موقعك الجغرافي وإلى أي دولة تنتمي. عناوين الآي بي مقسّمة عالميًا بين الدول وهناك لكل دولة مجموعة من عناوين الآي بي الخاصّة بها.

يمكنك زيارة موقع IPLocation.Net لمعرفة عنوان الآي بي الخاصّ بك، وستكتشف أن الموقع قادر على معرفة الدولة التي أنت قادم منها، ويمكنه كذلك تحديد موقعك الجغرافي وصولًا إلى المدينة التي أنت بها وأحيانًا الحيّ الذي تقيم فيه.

عنوان الآي بي الخاص بك مرتبط بالاشتراك الذي تحصل عليه من مزوّد خدمة الإنترنت في بلدك. فمثلًا عندما تشترك بمزوّد خدمة الإنترنت الوطني في مصر، يمكن لذلك المزوّد أن يمتلك معلومات عن مواقع الويب التي تزورها ونشاطك على شبكة الإنترنت، لأنّ عنوان الآي بي الخاص بك مرتبط باشتراكك الذي تدفعه شهريًا هناك.

عنوان الآي بي غالبًا ما يتغير بصورة مستمرة لكل مستخدم مشترك في مزوّد خدمة الإنترنت. فمثلًا قد يكون عنوان الآي بي الخاص بك اليوم هو 216.3.128.12، وغدًا قد يصبح فجأة 88.3.128.12، خصوصًا عندما تقوم بإعادة تشغيل الموجه (Router، أو يقال له راوتر) الخاص بشبكتك.

2. 10. نظام أسماء النطاقات (DNS)

كذلك كما شرحنا سابقًا فإنّ نظام أسماء النطاقات هو عبارة عن نظام يُوصل عناوين الآي بي بأسماء النطاقات (Domain Names) المُقابلة لها، وهو مهمّ جدًا في عمل الإنترنت.

عندما تتصل بالإنترنت فإنّك تستخدم نظام DNS الخاص بمزوّد خدمة الإنترنت الذي تستعمله. لذلك يمكن بسهولة لمزوّد خدمة الإنترنت الخاص بك أن يعرف ما هي مواقع الويب التي تزورها، لأنّه قادر على استلام طلباتك وتسجيلها، بالتالي هو يعرف أنت ماذا تطلب. لكن يمكنك تغيير نظام أسماء النطاقات الذي تستعمله متى ما تشاء، والعملية ليست صعبة بل سهلة عمومًا. هناك الكثير من الخدمات والمؤسسات والشركات التي تقدّم خدمة DNS مجانية وتحترم الخصوصية ولا تتبع لحكومة معيّنة.

قد يدور في ذهنك سؤال: «وما المشكلة في معرفتهم أسماء المواقع التي أزورها فقط»؟ في الواقع، هذه مشكلة كبيرة، تخيّل مثلًا أنّ مزود خدمة الإنترنت قد علم أنك تزور هذه المواقع بهذه التواريخ:

google.com [18:34:44 2020/03/09]
wikipedia.org [18:35:23 2020/03/09]
pregnancybirthbaby.org.au [18:42:29 2020/03/09]
maps.google.com [19:02:12 2020/03/09]

سيفهم الآن أي شخص يعمل في أيّ مزوّد خدمة إنترنت أنّك كنتَ تبحث عن شيءٍ متعلّق بالأمومة أو الإجهاض أو ما شابه ذلك، وهذا لأنّك زرت ويكيبيديا أوّلًا عبر البحث من جوجل، ثمّ وصلت إلى موقع pregnancybirthbaby.org.au (وهو موقع يتعلق بالأمومة ورعاية الأطفال في أستراليا)، وقد فتحت خرائط جوجل وهذا يعني أنّك كنت تبحث عن مواقع قريبة منك إمّا لمستشفيات أو مستوصفات أو أماكن لها علاقة برعاية الأطفال والأمومة أو الإجهاض.

وهكذا عبر بضعة أسطر فقط من سجّل الـDNS يمكن كشف الكثير من المعلومات عنك.

2. 11. الجدار الناري

الجدار الناري (Firewall) هو طبقة عازلة لنظام التشغيل، تسمح له بالتحكّم بالاتصالات التي تجريها البرامج والخدمات المثبّتة والسماح لها أو منعها. حيث قد يسمح الجدار الناري لبعض الخدمات بالاتصال بالإنترنت مثلًا أو منعها بناءً على مجموعة قواعد أو إعدادات معيّنة. الجدار الناري مهم للأمان فهو ينظّم الاتصالات بالشبكات الخارجية مع التطبيقات المحلّية على النظام أو الخادوم، ومن دونه قد يبقى الأمر مفتوحًا للعالم الخارجي ليصلوا إلى حاسوبك أو شبكتك أو خادومك، ولذلك من المهمّ التأكّد من تفعيله.

على ويندوز مثلًا، الجدار الناري يأتي مفعلًا افتراضيًا وسيعرض لك رسالة تحذير إن حاول

برنامج أو خدمة الاتصال بموقع إنترنت خارجي على شبكة إنترنت عمومية (شبكة المطارات مثلًا). والجدران النارية أنواعٌ شتّى وكلٌ منه له مميزاته الخاصّة.

تستفيد الخواديم بصورة كبيرة من الجدران النارية، فهي أحد الدعامات الأساسية في حمايتها من المتطفلين والمخترقين، وتمنعهم من الوصول إلى الخدمات الحسّاسة التي يجب ألّا يصل إليها أحد من خارج الخادوم نفسه.

توظّف الجدران النارية ما يُعرف بالمنافذ (Ports) وهي مثل «أبواب الولوج» إلى النظام، قد يصل عددها إلى 65 ألف منفذ افتراضي ممكن. تُستعمل المنافذ من قبل الخدمات المختلفة العاملة على نظام التشغيل حيث يقيم كلٌ منها على منفذ معيّن لا يُسمح بالتشارك فيه. فإذا أردت الوصول إلى خادوم البريد المحلّي المثبّت على الجهاز مثلًا فقد تجده على المنفذ 443 (تمثَّل تلك المنافذ بالأرقام)، وهكذا كل خدمة لها منفذها الخاص.

2. 12. بروتوكولات HTTP وHTTPS وغيرها

إنّ إرسال واستقبال البيانات ما بين حاسوبك المحمول وهاتف الذكي، وبين خواديم مواقع الإنترنت (Servers) يتم عن طريق ما يُعرف بالبروتوكولات (Protocols). البروتوكولات ببساطة هي طريقة تواصل وتخاطب بين الأجهزة بمختلف أنواعها، وهناك نوعان رئيسيان منها:

1. HTTP: وهو أحد عظام الرقبة للإنترنت. يقوم هذا البروتوكول على مرحلتين أساسيتين: إرسال الطلبات (Requests) إلى الخواديم، ثم إرجاع الرد (Response) إلى المُرسِل. تحوي الطلبات على معلومات عن المُرسل وكذلك الصفحة أو الرابط الذي يريد الوصول إليه، كما يحوي الرّد على معلومات عن المُستقبِل بالإضافة إلى المعلومات والبيانات التي يطلبها المُرسل.

2. HTTPS: وهو نفس البروتوكول السابق، لكن مع استعمال التشفير. يُعتبر هذا البروتوكول أكثر أمانًا بكثير من سابقه، ويجب أن تستخدمه المؤسسات البنكية والتعاملات الحساسة طوال الوقت، فهو يمنع أي طرفٍ خارجي عدا عن المُستخدم وصاحب الموقع من الوصول إلى البيانات التي يتم تداولها بينهما. هناك مبادرات ضخمة وعملاقة لتحويل الويب بأكمله إلى بروتوكول HTTPS عوضًا عن HTTP لأسباب تتعلق بالأمان والخصوصية، مثل Let's Encrypt.

هناك العديد من البروتوكولات الأخرى التي تُستخدم لأغراضٍ أخرى كذلك على الشبكة، مثل FTP (لتناقل الملفّات وتوزيعها) وSMTP (لإدارة البريد الإلكتروني الآمن).

2. 13. لغات برمجة الويب

بروتوكول HTTP (وكذلك HTTPS الذي ما هو إلّا تفريعٌ عنه) يستخدم لغة HTML للتواصل بين مختلف الأجهزة. HTML هي لغة بناء هيكلة مواقع وهي اللبنة الأساسية للإنترنت، كل الصفحات التي تتصفحها وتقرأها على الإنترنت مكتوبة باستخدام HTML، وهذا لأنّها لغة التواصل بين الخواديم وبين متصفّحات الويب مثل فيرفكس وجوجل كروم.

لغة HTML ليست لغة برمجة، بل هي لغة تواصل. على سبيل المثال الشفرة التالية:

```
<html>

<head>
    <title>Test</title>
</head>

<body>
    <a href=»https://google.com>Google</a>
</body>


</html>
```

يرسلها خادوم الويب إلى جهازك أو هاتفك الذكي، فيفهم متصفّح الإنترنت الخاص بك أنّ خادوم الويب يريد في الواقع عرض رابط بنص «Google» يشير إلى موقع جوجل في الصفحة، كما يفهم أنّك تريد استخدام كلمة Test كعنوان لتلك الصفحة، فيقوم هو من طرفه بعرض المحتوى لك بالشكل المطلوب.

جافاسكربت (JavaScript) هي لغة برمجة للويب، تسمح بالقيام بالكثير من العمليات بسرعة وعرض المحتوى بمختلف الطرق، وهي البنية التحتية الحقيقية لبناء صفحات الويب التي تراها. تستعمل معظم المواقع حول العالم شِفرات جافاسكربت في عملها. وهذه الشِفرات مثل البرامج؛ قد تكون آمنة وقد تكون خبيثة.

CSS هي لغة تصميم للمحتوى، فمثلًا إذا كنت تغيير الألوان أو التنسيق أو تصميم الصفحات، فعليك استخدام لغة CSS لتتمكن من ذلك.

يشكّل الثلاثي HTML/JavaScript/CSS طريقة التواصل المعيارية على الإنترنت. مواقع الإنترنت تقوم بإرسال هذه الملفّات التي تكون مكتوبة بطريقة معيّنة لضمان ظهور الموقع بالشكل الذي يريده مطورو ومبرمجو المواقع إلى متصفّحك، وهو بدوره يقوم بعرضها. ستحتاج هذه المفاهيم لاحقًا في الفصول المتقدّمة حيث سنتحدث عن صفحات الويب المزوّرة وحقن شِفرات جافاسكربت وغير ذلك.

2. 14. ختام الفصل

لقد شرحنا أهمّ المفاهيم الأساسية حول الحواسيب والشبكات والأجهزة في هذا الفصل.

إن أردت الاستزادة حول هذه المفاهيم فيمكنك ببساطة البحث عنّها في أيّ محرّك بحث أو مشاهدة الفيديوهات عنها على يوتيوب أو القراءة عنها على ويكيبيديا. من المهمّ أن تمتلك فهمًا جيّدا لهذه الأسماء والمصطلحات فهي أساسية لفهمك للأقسام الأخرى في كتاب دليل الأمان الرقمي.

3. الوعي في العالم الرقمي

سيشرح هذا الفصل أهمية الوعي في الأمان الرقمي والحفاظ على الخصوصية، ولماذا هو أهم شيء قد تمتلكه أن أردت الدخول في هذا المجال، الأمان الرقمي والحفاظ على الخصوصية. كما سيشرح بعض النصائح النظرية للحصول على مستوٍ عالٍ من الأمان.

3. 1. مفاهيم أساسية للوعي

الوعي صفة غير موضوعية لا يوجد تعريفٌ مشترك لها. لكن يمكن تعريف الوعي - في هذا المجال - بصورة عامّة أنّه الأسلوب الذي يتبعه المُستخدم في كل تصرّفاته في العالم الرقمي ليضمن حفاظه على أمانه وخصوصيته بالشكل الذي يريده ويرتضيه. المستخدم الواعي هو من يتبع مجموعة من الإرشادات والقواعد والأساليب المدروسة بصورة صحيحة أثناء استخدامه للأجهزة الرقمية، والمستخدم غير الواعي هو من لا يبالي بذلك.

الوعي مَلَكة من الصعب تعلّمها، وهذا لأنّه ليس شيئًا يمكن شرحه كبرنامج أو إضافة متصفّح مثلًا، بل هو أسلوب تفكير وتحليل للمعطيات، فهو مشتقٌ من ذكاء الإنسان وقدرته على التفكير. ولا يُمكن الإشارة للوعي بصورة مباشرة وأن يُقال: هذا هو الوعي فتعلّموه، بل على المرء أن يتعلمه بنفسه ويبنيه مع الزمن.

وهو أهم وسيلة دفاع ليمتلكها المُستخدم أثناء قيامه بأيّ عملٍ رقمي، ولهذا جعلناه في مقدّمة هذا الكتاب وقبل الفصول التطبيقية الأخرى، لأنّ كل تلك الأساليب العملية لن تجديك نفعًا إن لم تمتلك المعارف والمهارات والخبرات التي تؤهلك للقيام بها على أكمل وجه، ثم متابعة القيام بها.

ما قد يغذّي خزّان الوعي للقارئ هو أن يبحث في المصادر المتوفّرة على الشبكة عن مواضيع متفرقة في علوم الحاسوب؛ كيف يعمل الحاسوب والشبكات والهواتف والأنظمة المختلفة، وما هي

آخر الأخبار في مجال الأمان الرقمي والخصوصية، وما هي آخر الطرق التي استعملها المخترقون ووكالات التجسس للتنصت على المستخدمين وغير ذلك من المواضيع المتعلّقة بالمجال. يصبح القارئ تدريجيًا واعيًا بكل هذه الأشياء المحيطة به مع مرور الوقت.

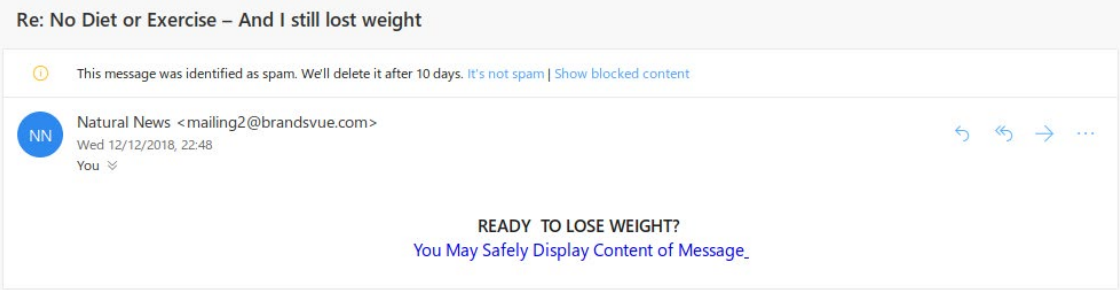
إليك جملة من النصائح العامة حول أشياء يجب عليك فعلها أو تجنبها من أجل الأمان الرقمي. هذه النصائح مجرّد خطوط عامة لأمور متكررة الحدوث، وليست تفصيلية:

1. احرص دومًا على الحصول على النسخ الأصلية من البرمجيات التي تستعملها. يقوم الكثير من الناس باستخدام برمجيات مُقرصنة (عبر التلاعب بها باستعمال برمجيات تدعى Crack) ظانّين أنه لا يوجد بها شيء، والواقع أنّ معظم هذه البرمجيات تحتوي على برمجيات تجسس أو عرض إعلانات أو إرسال بيانات خفية لا تشعر أنت كمستخدم بها. وهذا واحدٌ من الأسباب التي نستحسن بسببها البرمجيات المفتوحة المصدر (Open Source).

2. لا تقم بتاتًا بتحميل أي برنامج أو ملف من جهة لا تعرفها. يقوم البعض بتحميل برامج ويندوز مثلًا من مواقع كـCNET وغيرها من المواقع الموجودة على الإنترنت، والحاصل هو أن كل هذه البرامج التي تقوم بتحميلها من هذه المواقع تحتوي على برمجيات تتبع لنشاطاتك أو برامج إعلانات أنت في غنىً عنها. لذلك حاول دومًا الحصول على البرامج فقط من مزوّد نظام التشغيل الخاص بك (متجر برامج ويندوز وماك، متجر iTunes وGoogle Play، المستودعات الرسمية في لينكس... إلخ)، أو من المواقع الرسمية لتلك التطبيقات.

3. جميع رسائل البريد الإلكتروني التي تصلك والتي تقول لك أنّك ربحت مبلغ كذا، أو تطلب منك الانضمام لمشروع بنك إفريقي، أو تطلب منك معلومات شخصية عمومًا، أو تطلب منك أن تُراسلهم، تكون هذه الرسائل هي رسائل خداع يرسلها ضعفاء النفوس لمحاولة الاحتيال على الناس. لا تقم حتّى بفتحها ولا الرد على مُرسليها، فقط أرسلها إلى مجلّد السخام أو السبام spam.

4. تأتي الكثير من رسائل الاحتيال الإلكتروني بملفّات مرفقة. فيقول لك المُرسل: "افتح الملف المُرفق لمزيد من المعلومات"، والحاصل هو أنّ الملفّات المرفقة هذه تكون محمّلة بفيروس يمكن أن يتسبب باختراقك وسرقة معلوماتك دون أن تشعر. قد تكون الشفرة الخبيثة أو الفيروس موجودة في الرسالة نفسها كمحتوى HTML، ويطلب منك عرضها، تجنب القيام بذلك.



5. تأكّد من أن عنوان الويب (URL) في متصفّحك هو مطابق للموقع الذي تريد فتحه. تقوم مثلًا بعض رسائل البريد الإلكتروني بتحويلك إلى موقع مثل facebok.com، وعندما تفتح الصفحة ستجد واجهة شبيهة جدًا بواجهة موقع فيس بوك، فتقوم أنت بإدخال اسم المستخدم وكلمة المرور ظانًّا أنّ هذا هو موقع فيس بوك الحقيقي، ثم يُخترَق حسابك مباشرةً لأنّهم قد حصلوا على بياناتك. لأنّ موقع facebok.com ليس هو نفسه facebook.com ولا يتبع له، بل هو موقع تابع للمُخترِقين مثلًا، وكل البيانات التي تُدخلها هناك سوف تصل إليهم. يُعرف هذا بالتصيد الاحتيالي (Phishing).

6. تتيح معظم مواقع الإنترنت ميّزة الحفاظ على تسجيل الدخول (Stay Signed-In)، وهو غالبًا ما يستعمله معظم المستخدمين لتجنّب إدخال اسم المستخدم وكلمة المرور في كلّ مرة يفتحون به الموقع. لهذا انتبه إلى عنوان موقع الويب الحالي إذا ما طُلب منك إدخال اسم المستخدم وكلمة المرور، فالمُفترض ألّا يحصل ذلك عادةً، وربّما يكون موقعًا مزوّرًا وليس الموقع الذي تريد زيارته.

7. لا تشارك بياناتك الحساسة كاسم المُستخدم وكلمات المرور مع أي شخص، مهما كان السبب. حتّى لو كنتَ تثق به فالمشكلة ليست الثقة وحدها بل كيف سيؤمّن هو بياناتك هذه ويحميها من الاختراق كذلك.

8. إذا كنت لا تعرف شيئًا عن موضوع معين أو مشكلة، فاسأل من هم أكثر خبرةً منك عن الموضوع قبل أن تقدم على أي خيار. التصرّف لوحدك قد يتسبب لك بمشاكل إن لم تكن ذا خبرة.

9. فكّر قبل أن تتخذ أيّ إجراء.

3. 2. حول رفع بياناتك وملفاتك على الشبكة

ما لا يدركه الكثير من الناس عندما يشاركون أي شيء على مواقع التواصل - بل وحتّى غيرها من المواقع - أنّ معظمها تشترط إعطاء حقوق ملكية فكرية كاملة من طرفك لتلك المنصّة. فيس بوك مثلًا ينصّ على ذلك بوضوح في شروط الاستخدام الخاصّة به [1].

على وجه التحديد، عندما تقوم بمشاركة محتوى محمي بموجب حقوق الملكية الفكرية أو نشره أو تحميله على أو في منتجاتنا أو بأي طريقة ذات صلة بمنتجاتنا، فإنك بذلك تمنحنا ترخيصًا دوليًا غير حصري، قابلاً للنقل، وقابلاً للترخيص من الباطن، وغير محفوظ الحقوق، لاستضافة المحتوى، واستخدامه، وتوزيعه، وتعديله، وتشغيله، ونسخه، وتقديمه أو عرضه على العامة، وترجمته، وإنشاء أعمال مشتقة منه (بما يتوافق مع إعدادات الخصوصية والتطبيق الخاصة بك). وذلك يعني أنه، على سبيل المثال، إذا قمت بمشاركة صورة على فيسبوك، فإنك بذلك تمنحنا إذنًا يسمح لنا بالحق في تخزينها ونسخها ومشاركتها مع الآخرين (ونكرر، بما يتوافق مع إعداداتك) مثل موفري الخدمات الذين يدعمون خدمتنا أو غير ذلك من منتجات فيسبوك التي تستخدمها. وتنتهي صلاحية هذا الترخيص بمجرد حذف المحتوى الخاص بك من أنظمتنا.

تستعمل الشركات الأخرى مثل جوجل الصور التي ترفعها كبياناتٍ لتدريب أنظمة الذكاء الصناعي الخاصّة بها، حيث تُستعمل صورك من أجل تدريبها على التقاط بعض العناصر أو التعرّف عليها، مما يساعد جوجل في تقديم خدمات تجارية لاحقًا للشركات الأخرى [2].

من خلال تسليم أو نشر أو عرض المحتويات، فإنك تمنح Google ترخيصاً دائماً وغير قابلٍ للنقض وفي كل أنحاء العالم وبدون رسوم وغير حصري بإعادة إنتاج وتكييف وتعديل وترجمة ونشر وإنجاز علناً وعرض علناً وتوزيع أي من المحتويات التي تسلمها أو تنشرها أو تعرضها في أو من خلال الخدمات. وهذا الترخيص هو فقط لغرض تمكين Google من عرض وتوزيع وترويج الخدمات ويمكن سحبه بالنسبة لخدمات معينة كما هو محدد ضمن الشروط الإضافية لتلك الخدمات.

مشاركتك على موقع Reddit مثلًا تعطي الحق لكل المستخدمين - وليس فقط مدراء موقع Reddit - بأن يستخدموا محتواك ويعدّلوه ويعيدوا مشاركته بأي طريقةٍ شاؤوا طالما أنهم يشيرون إلى مساهمتك الأصلية ولا يستعملونها بصورة تجارية.

كل المنصّات الرقمية تطلب منك إذنًا شبيهًا عندما تقوم باستخدامها، والمشكلة هي أنّ المستخدم غالبًا ما يوافق على شروط الاستخدام دون أن يقرأ المكتوب فيها.

هـذا بالنسـبة لتعاملـك مـن ناحيـة الشـركات الموفّـرة للخدمـات، لكـن مـن ناحيـة الأفـراد فالأمـر أصعب، لأنّ الأفراد قادرون على جمع معلوماتك وصورك، وحفظها في مجلّدٍ على أجهزتهم الشخصية وعدم إخبار أي أحد بذلك. ولن تعرف حتّى من هم ولماذا يحتفظون ببياناتك عندهم.

لأجل هذا عليك اعتبار كل ما ترفعه على الشبكة من بيانات وملفّات صار منتشرًا عند كل الناس، ولا رجعة فيه. لذلك فكّر مرتين قبل أن ترفع صورك الشخصية أو تعلن عن آرائك الفكرية والسياسية في أي مكان، فلا تدري متى يخرج أحدهم بها ليحاول استخدامها ضدك.

3. 3. شيء مرعب ما يمكنني معرفته عنك

دعونا نستعرض ما يمكننا كأفراد معرفته عن بعضنا البعض عبر المعلومات التي ننشرها على الشبكة.

ما الحسابات والخدمات الرقمية التي يستخدمها أي مستخدم معاصر اليوم؟ لا بد من أن يستخدم بريدًا إلكترونيًا، وحساب فيس بوك وربما حساب تويتر أو حسابات على مواقع اجتماعية أخرى.

ما الذي يمكنني معرفته عنك عبر حسابك على فيس بوك؟ يمكنني رؤية المنشورات العامّة التي تنشرها من نصوص وصور وفيديوهات، كما يمكنني غالبًا رؤية قائمة أصدقائك، والناس الذي يعلّقون عندك ويتفاعلون مع منشوراتك بالإعجابات والتعليقات والمشاركات. كان يمكنني ألّا أرى شيئًا من هذا إن استخدمت إعدادات الخصوصية المناسبة، لكن للأسف معظم المستخدمين لا يستخدمونها ويتركون كل شيءٍ ليكون مكشوفًا للعموم.

الآن إليك بعض الأشياء التي يمكنني معرفتها عنك عبر فيس بوك:

- يمكنني استخدام مربّع البحث في فيس بوك لرؤية كل الصور أو الفيديوهات التي رفعتَها أنت، أو رفعها أحدٌ آخر وأشار فيها إليك. مربّع البحث في فيس بوك لا يعرض لي المنشورات النصية فقط، بل يعرض لي الصور والفيديوهات كذلك إن أردت البحث عنها. كما يمكنني فلترتها حسب المدة الزمنية.
- يمكنني استخدام نفس مربع البحث للبحث عن اسمك، ورؤية كل التعليقات العامة التي أجريتها على فيس بوك وكل المنشورات العامة التي نشرتَها في أي مكان منذ تاريخ انضمامك إلى فيس بوك. يشمل هذا المنشورات التي تنشرها داخل مجموعات فيس بوك المختلفة، حيث يمكنني رؤيتها جميعًا عبر البحث عن اسمك في فيس بوك (إن كان المجموعات عامّة، أو

حتّى لو كانت خاصّة أو سرّية إن كنتُ أنا أيضًا عضوًا فيها). يسمح فيس بوك لي كذلك برؤية كل المنشورات التي نشرتَها في مجموعة معينة منذ انضمامكَ إليها إن أردتُ ذلك.

- يمكنني تصفّح قائمة أصدقائك وفتح حساباتهم. ويمكنني الآن استعراض قائمة الإعجابات على منشوراتهم لمعرفة ما يعجبك أنت مما ينشرونه لأعرف المزيد عنك وعن اهتماماتك. كما يمكنني رؤية أي منشورات أو تعليقات ينشرونها عنك أنت على حساباتهم الشخصية، مثل النزهات والمشاوير التي تقومون بها أو أي أعمال أخرى تقومون بها سويةً. يكثر هذا كثيرًا في الحسابات العائلية على فكرة، حيث ينشر الأب أو الأم الكثير من المعلومات عن أولادهما دون أن يدري الأولاد بذلك. فلمعرفة المزيد عنك قد لا أحتاج الوصول إلى حسابك الشخصي أنت والمعلومات المنشورة فيه، بل يكفيني الوصول إلى حسابات أقاربك ومعارفك وأصدقائك لأعرف المزيد عنك.

عبر تجميع كل هذه المعلومات مع بعضها البعض، يمكنني بناء ملف كامل حولك ومعرفة تفاصيل كنتَ لا تظن أن أيّ إنسانٍ غريبٍ عنك قد يعرفها. وقد تُستعمل هذه المعلومات لتعقّبك أو إبداء الأذية لك أو لاستغلالها ضدّك في نشاطاتٍ مختلفة من الحياة اليومية.

كلّ ما سبق كان عبر استخدام فيس بوك لوحده، لكن كلما ازدادت المنصّات والخدمات التي تستخدمها على الشبكة، ازدادت معها قدرة الآخرين على معرفة المزيد من المعلومات حولك. وأهم هذه المعلومات هي بريدك الإلكتروني.

يظن الكثير من الناس أنّه لا مشكلة في نشر بريده الإلكتروني على العلن، ففي النهاية ما الذي سيفعلون به؟ إنّه مجرد عنوان لاستقبال الرسائل! وهذا للأسف الشديد غير صحيح بالمرّة.

عنوان بريدك الإلكتروني سيكشف كامل هويتك الرقمية إن استعملته على أي منصّة رقمية تنشره. على سبيل المثال وهذا من تجربتي الشخصية، حيث كانت الجامعات في تركيا مثلًا تنشر ملفّات PDF بقوائم المقبولين والمرفوضين لديها كل سنة. وللأسف لا يمنعون فهرسة هذه الملفّات من قبل محركات البحث، فكانت هذه الملفّات تظهر بسهولة عند البحث عن اسم الشخص أو بريده الإلكتروني في جوجل، فتظهر لك كل الجامعات التركية التي أرسل لها صاحب البريد الإلكتروني هذا طلب قبولٍ لديها!

ستظهر كل الخدمات الأخرى التي تعرض بريدك الإلكتروني للعلن عند البحث عنها في أي محرك بحث. وهكذا يُمكن لأي شخص أن يحصّل المزيد من المعلومات عنك.

ومن الأشياء المهم ملاحظتها حول البريد الإلكتروني هو أنّه عبر إزالة اسم البريد وعلامة @

منه (أي عبر البحث عن testuser بدلًا من testuser@outlook.com) ستظهر المزيد من النتائج عن معظم الناس في محرّكات البحث، وهذا لأن الكثير من الناس في الغالب يستخدمون نفس اسم المستخدم الخاص ببريدهم الإلكتروني كاسم مستخدم كذلك لحساباتهم على فيس بوك وتويتر وغيرها من الخدمات الأخرى. وهذا ما يسبب سهولة العثور عليها جميعًا في نفس عملية البحث.

تويتر قصّة أخرى. إذا كان لديك حساب على تويتر فيمكن لأي إنسان أن يستعرض التغريدات التي قمتَ أنت بالإعجاب بها، أو قمتَ بالرد عليها من حسابك على تويتر مباشرةً. يُمكن كذلك عبر ميّزة البحث المتقدم في تويتر أن يستعرض أي إنسان ردودك على ردود حسابات معيّنة؛ فإذا كنت تتفاعل بكثرة مع حساب معيّن مثلًا وقد لاحظ الشخص الذي يبحث عن معلوماتك هذا، فحينها يمكنه أن يقرر رؤية ردودك على تغريدات ذاك المستخدم بالتحديد.

وكما الأمر في كلّ المنصات الاجتماعية، حيث لا يمكنك منع الآخرين من الحديث عنك. ربّما قام حساب الجامعة الرسمي التي تدرس فيها مثلًا أو حساب الشركة التي تعمل فيها أو حساب لأي شخص آخر بنشر صورة تكونُ موجودًا فيها ويَذكر اسمك أيضًا. فهكذا تصبح صورك ومعلوماتك متوفرة بيد الآخرين دون أن يكون لك يد في الموضوع. وبمجرّد البحث عن اسمك في أي محرّك بحث فستظهر معلوماتك.

هناك أيضًا محرّكات بحث متخصصة للبحث عن أشخاص أو بيانات معينة لهم، على عكس محركات البحث العامّة مثل جوجل وبينغ Bing مثلًا، فلا تظن أنّه بمجرد عدم العثور على نتائج عنك على جوجل فإنه لا يوجد شيءٌ عنك كذلك.

عليك الحرص كذلك على التعليقات والمقالات التي تنشرها في الشبكة، وخصوصًا التعليقات. يظن البعض أن التعليقات التي يكتبها على مواقع الإنترنت سواءٌ العربية منها أم الأجنبية لا يمكن الوصول إليها سوى عبر المقال نفسه، لكن محرّكات البحث تؤرشفها كذلك. ولهذا فإنّ كل التعليقات التي تدلي بها على المدونات والموسوعات والمواقع الإلكترونية الأخرى... كلّها ستكون ظاهرة عبر البحث عن اسمك.

سنتحدث في الفصل اللاحق عن ضرورة استخدام أسماء وهمية في بعض المنصّات وعدم استخدام الاسم الحقيقي. لكن نريد التنويه بصورة سريعة هنا إلى أن كل الحسابات التي تستخدمها على الشبكة وتستعمل فيها نفس الاسم هي حسابات عليك أن تعتبرها بيد كل الناس الذين تراهم في الشارع حولك. لأنّهم جميعًا قادرون على الوصول إليها عبر مجرد البحث عن اسمك بالإنجليزية أو العربية أو أي لغة أخرى.

3. 4. هوية الإنترنت الوهمية

من الأمور التي يقوم الكثير من الناس بها هي أنهم يفصلون بين هويّاتهم المختلفة على الإنترنت. فتجدهم عندما يتصفّحون مواقع مثل رِديت Reddit أو حتى فيس بوك وتويتر، يستعملون أسماء وبيانات وهمية لا تعبّر عن هويتهم الحقيقية. بعضهم يفصل بين الحياة المهنية والترفيهية، وبعضهم يستعمل أسماءً وهمية للحديث في مواضيع جدلية في بعض الأماكن وغير ذلك.

عليك أنت أن تقرر كذلك ما نوعية الهوية التي تريد استخدامها على الإنترنت؟ الهوية الوهمية تمنحك خصوصية وأمانًا أكبر، فالآن اسمك صار وهميًا ولا أحد يعرف من أنت (باستثناء الدولة التي تعيش بها بالطبع، لأنّك تستعمل مزوّد خدمة الإنترنت الخاص بها، ما لم تقم بإجراءات للتخلص من ذلك، وباستثناء المنصّة أو الخدمة التي تتصفحها فهي لديها عنوان الآي بي الحقيقي الخاص بك، ويمكن لهذين الاثنين أن يتعاونا لكشف هويتك).

إنّك بالطبع تخسر الكثير عندما تشارك على الإنترنت بأسماء وهمية (إنشاء علاقات مع الآخرين باسمك الحقيقي، ونسب مساهماتك لك أنت ونشر اسمك بين الناس.. إلخ)، لكن فكّر في عواقب ما تنشره كذلك وهل من المناسب أن يلتصق باسمك وهويتك الحقيقية أم لا؟ إن كان الجواب لا، فحينها عليك استخدام هوية وهمية، والقيام بعددٍ من الإجراءات الأخرى كذلك لحماية نفسك. تذكّر أن الاسم الوهمي لا يحميك لا من الدولة التي تعيش بها ولا من صاحب الخدمة أو الموقع الذي تزوره والسبب أن تمتلك الخدمة أو المنصّة أو موقع الويب الذي تزوره عنوان الآي بي الخاص بك كذلك. وما يفعله الكثير من الناس هو أنهم يقومون بإنشاء حسابين اثنين أحدهما لهويتهم الحقيقية والآخر لهويتهم الوهمية، لكنهم يفعلون ذلك من نفس الجهاز ونفس عنوان الآي بي، وهو ما يعني نظريًا أنّ لدى أصحاب تلك المواقع القدرة أن يعرفوا أنّ هذين الحسابين يعودان لنفس الشخص، فهما قد قاما بتسجيل الدخول من نفس عنوان الآي بي. مجرد تسجيلك/تسجيل الدخول ولو لمرّة واحدة بنفس عنوان الآي بي للحسابين سيكون كافيًا لكشف هويتك.

3. 5. تقييم المخاطر والرغبة في الحماية

عليك الآن أن تتخذ قرارًا حول درجة الأمان والخصوصية التي تريد الحفاظ عليها. هل تريد مثلًا ألّا يكون هناك أي معلومة أو صورة عنك على الإنترنت على الإطلاق؟ هل تريد أن تفصل حياتك المهنية عن حياتك الترفيهية وتستعمل أسماء وهمية مختلفة؟ هل تخاف من نشر مقالٍ ما لأيّ سببٍ من الأسباب؟ هل أنت على وشك الدخول للسياسة حيث كل معلومة بسيطة عنك قد تُستخدم ضدك في المستقبل من المنافسين؟

الكل عليه محاولة الحفاظ على أمانه الرقمي، لكن إلى أي درجة؟ هذا يختلف بالطبع حسب حالتك. وهذا مهم لأن طرق الحماية والتأمين ستختلف كذلك، وكلّما أردت حماية وخصوصية أعلى، كانت التكاليف من وقت وجهد وصعوبة في الاستخدام أعلى وأكثر.

ومن المهم كذلك أن تحدد ضد من تريد الحماية؟ هل تريد حماية نفسك من الشركات الأجنبية التي تستعمل خدماتها مثل فيس بوك وجوجل، أم من الأفراد والمخترقين الخارجيين، أم من أصحاب المواقع التي تزورها، أم من ماذا بالتحديد؟ من الذي يزعجك ويخيفك من بين هؤلاء؟

لجعل الموضوع أكثر بساطةً، فكّر بهدوء ثمّ أجب عن الأسئلة التالية:

- ضد من أريد حماية نفسي؟
- ما هي نوعية المعلومات التي لا أريدها أن تتوفر لدى شخصٍ آخر بتاتًا؟
- ما هي نوعية المعلومات التي لا مشكلة لدي في أن تُنشر عنّي؟
- هل نشر هذه المعلومات عنّي بعد 5 أو 20 أو 30 سنة من الآن لن يكون مشكلًا كذلك؟
- إلى أي مدى أنا مستعد لدفع المال والجهد والوقت للوصول إلى درجة الحماية التي أريدها؟

إجابتك على الأسئلة السابقة مهمة وأنت تستعرض فصول هذا الكتاب، حيث سيجب عليك أن تقرر بنفسك: "هل هذا شيء أريد تطبيقه أم لست بحاجته في حالتي"؟

تذكّر دومًا أن الخصوصية والأمان لا يأتيان بالمجان دون مجهود أو تعب.

3. 6. ختام الفصل

الوعي مهم جدًا في كل نشاطاتك التي ستقوم بها عبر الشبكة، وهو أوّل طبقة حماية وأمان لك أمام العالم الخارجي. تذكّر أنّ هذه النصائح كانت لوضعك على بداية الطريق فقط، أمّا الباقي، من تعلّم المزيد من المفاهيم وتجنّب الأخطاء الشائعة هو عليك أنت.

4. اختيار العتاد والبرامج

سيقدم هذا الفصل أهمّ الأساليب المتبعة حاليًا في صناعة البرمجيات والعتاد، وكيفية الاختيار والتفاضل بينها. كما سيشرح أهمية تحديثات البرمجيات بالإضافة إلى تقديم عددٍ من البرمجيات البديلة المفيدة للمستخدم.

4. 1. ما بين البرمجيات المفتوحة والمغلقة

كما ذكرنا في فصل المفاهيم التأسيسية، فإنّ البرمجيات المغلقة (Closed-Source Software) هي تلك التي لا تسمح لك بتعديل ورؤية ومشاركة الشِفرة المصدرية للبرنامج، بل تتطلب موافقتك على شروط استخدام معيّنة (End-User License Agreement) قبل أن تتمكن من استخدام البرنامج. بينما البرمجيات المفتوحة (Open-Source Software) هي تلك التي تسمح لك بتعديل ورؤية ومشاركة الشِفرة المصدرية للبرنامج دون قيودٍ بصورة عامّة (إلّا القيود المتعلّقة بأحد تراخيص البرمجيات المفتوحة، مثل أنّه عليك ذكر أسماء المطورين الأصليين وتوزيع برنامجك المُشتَق كذلك تحت نفس الرخصة ...إلخ).

الكثير من البرمجيات التي تراها حولك هي مفتوحة المصدر، مثل متصفّح فيرفكس للويب ونظام لينكس وتوزيعاته، وبرنامج عارض الفيديو VLC وغيرها الكثير من البرامج. نواة نظام أندرويد الموجود على هاتفك مفتوحة المصدر فهي نواة نظام لينكس نفسها.

مهما كان تصنيف البرمجيات التي تستعملها، عليك أن تحاول دومًا الاعتماد على البرمجيات المفتوحة، للأسباب التالية:

- البرمجيات المفتوحة تتيح لك ولغيرك رؤية الشفرة المصدرية، وهذا يضمن قدرتكم على التحقق من خلوها من برمجيات التجسس والأبواب الخلفية. وهذا لا ضمن خلوّها منها، بل

يضمن قدرتكم على التحقق من ذلك فقط، فإن لم يقم أي شخص بفعل ذلك فحينها لا يوجد ضمان أنّ هذا البرنامج آمن بالطبع.

- صحيحٌ أنّ كون البرمجيات مفتوحة لا يعني كونها مجانية طوال الوقت، لكن في معظم الأحيان البرمجيات المفتوحة مجانية تمامًا في الواقع. وهذا أفضل - من الناحية المادّية وحساب التكلفة - على المدى البعيد خصوصًا مقابل البرمجيات المغلقة التي تتطلب اشتراكًا شهريًا، مثلًا برمجيات أدوبي (Adobe) مثلًا.
- يستخدم الكثير من الناس برامج كسر الحماية (Crack) للحصول على البرمجيات المدفوعة المغلقة المصدر مجانًا، لكنّ هذه البرامج مليئة معظم الأحيان ببرمجيات التجسس وعرض الإعلانات وسحب البيانات من جهازك دون أن تشعر. استعمل البرمجيات المفتوحة بدلًا من أن تلجأ لهذا الطريق.
- تمتلك البرمجيات المفتوحة مجتمعاتٍ كبيرة وراءها عادةً. وهذا يعني أنّك كمستخدم قادر على الحصول على الدعم والمساعدة من مطوري هذه البرمجيات والمستخدمين الآخرين الذين يستعملونها، على عكس البرمجيات المغلقة التي لم تدفع ثمنها.
- لدى البرمجيات المفتوحة القدرة على الاستمرارية حتّى لو توقّف مطوروا المشروع عن تطويرها، على عكس المغلقة المصدر. وهذا لأنّ الشِفرة المصدرية مفتوحة وبإمكان أي شخص أن يأخذها ويتابع تطويرها بنفسه. وهو ما يعطيك كمستخدم أمانًا من ناحية استمرارية هذه البرمجيات وعدم اختفائها بين يوم وليلة.

هذا لا يعني بالطبع أنّ كل البرمجيات المغلقة لها بدائل أفضل منها من البرمجيات المفتوحة، ولكن إذا تساوت لديك المزايا فحينها عليك بالطبع ترجيح المفتوح المصدر منها.

4. 2. اختيار العتاد

العتاد (Hardware) في عصرنا الحالي قصّة مؤسفة، إذ يأتي معظمه من شركات صينية أو أمريكية أو أوروبية، ولا يمكنك أنت كمستخدم عربي التوقّف عن الشراء منهم فليس لدينا بديل عربي مناسب لهذه الأجهزة، وبالتالي لا يمكنك أن تضمن كفرد أنّ العتاد الذي تشتريه خالٍ من برمجيات التجسس والمراقبة.

نعم، يمكن للعتاد كذلك أن يحتوي برمجيات تجسس محمّلة مسبقًا. قامت شركة لينوفو (Lenovo) الشهيرة مثلًا سنة 2015م بشحن مئات الآلاف من الحواسيب المحمولة التي تحوي

برمجيات تجسس محمّلة مسبقًا [1]. كما تُكتشف على مدار الشهور العشرات من الشركات الصينية التي تبيع الهواتف المحمولة الرخيصة على أنّها كانت تشحن برمجيات تجسس داخل تلك الهواتف كذلك. أبرزها كان ما اكتُشف سنة 2016م عن 700 مليون هاتف أندرويد قادم من الصين مع برمجيات تجسس خبيثة ترسل كل بيانات المستخدمين كل 72 ساعة [2]. هل عرفت الآن لماذا تلك الهواتف رخيصة؟

تأتي المشكلة الأكبر بخصوص العتاد عند الهواتف المحمولة؛ تأتي جميع الهواتف بنظام تشغيل محمّل مسبقًا ولا يمكنك استبداله (مثل أندرويد وiOS). الكثير منها يسمح لك بعمل ما يعرف بالصلاحيات المطلقة "روووت" (Root) للجهاز حيث يصبح بإمكانك امتلاك كامل الصلاحيات عليه ثم حذف نظام التشغيل الحالي وتثبيت نظام آخر مثلًا، لكن جميع الشركات تقول لك أنّك ستفقد ضمان الجهاز بمجرّد قيامك بهذه الخطوة، فتظل مجبورًا على استخدام نظام التشغيل القديم المليء بالبرمجيات التي لا تعرفها ولا تعرف ماذا تفعل على نظامك. هناك جزءٌ كبير من الهواتف المحمولة التي لا تسمح لك بعمل روووت للجهاز حتّى والتحكم الكامل بالهاتف.

هذا بالنسبة للمستخدمين، لكن المشكلة موجودة حتّى بالنسبة للشركات، فقد نشرت بلومبيرغ تقريرًا سنة 2019م عن قطعة عتاد صغيرة خبيثة ترسل بيانات حساسة للصين داخل معالجات أحد الشركات الصينية والتي تُصدَّر لتعمل داخل مراكز البيانات لشركات مثل أمازون وآبل في أمريكا [3]. علّقت كلّ الشركات أن التقرير غير صحيح بل وتدخلت وكالة الأمن القومي الأمريكية (NSA) لتقول أنّ التقرير عارٍ عن الصحّة. لكن وإن كان التقرير خاطئًا إلّا أنّه دفع المتخصصين في المجال للتأكيد على سهولة هذا النوع من الهجمات وإمكانيته، وأنّ الولايات المتحدة نفسها كانت تمارسه على مدار عقود للتجسس على الدول الأخرى [4].

ملخّص الكلام هو أنّه لا يمكنك كمستخدم التأكد تمامًا أنّ عتادك لا يوجد به قطعة من هذه القطع. وعليك أنت كمستخدم أن تقرر أي درجة من الحماية والخصوصية تريد أن تمتلك من ناحية العتاد.

لكن ما لا يُدرك كلّه لا يترك جلّه. إليك بعض النصائح المتعلّقة بشراء العتاد:

- اشتري دومًا من شركات مشهورة مثل ديل (Dell) وآبل وغيرها. لا تشتري أجهزة الحواسيب والهواتف المحمولة من ماركات غير معروفة أو غير شهيرة.
- حاول شراء الحواسيب التي تأتي محمّلة مسبقًا بأحد توزيعات نظام لينكس، فهي عادةً ما تكون أرخص بـ100$ من تلك التي تأتي محمّلةً بويندوز (بسبب سعر الرخصة).

- إن كان العتاد رخيصًا لدرجة غير معقولة فحينها غالبًا بياناتك هي ما يكمل بقية السعر عبر تجميعها وبيعها لاحقًا.
- عندما تشتري حاسوبًا جديدًا، احذف نظام التشغيل الموجود عليه بالكامل وقم بتثبيته بنفسك من جديد. لا يمكنك أخذ كلمة الشركة المصنّعة بخصوص ما يوجد على حاسوبك مسبقًا، فالحل الأنسب هو أن تحذف كل شيء وتثبّت نظامك بنفسك.
- احذف كل التطبيقات الافتراضية التي تأتي على هاتفك المحمول الجديد أو على الأقل عطّلها، ثم ثبّت التطبيقات التي تحتاج إليها فقط.
- تابع دومًا آخر أخبار الحماية والأمان والخصوصية المتعلّقة بالعتاد، لترى ما إذا كان أحد الأجهزة التي تمتلكها مشتبهًا به أنّه يحوي برمجيات تجسس.

4. 3. العتاد المتخصص بحفظ الخصوصية

بسبب كل ما سبق من انتهاكات الخصوصية من ناحية العتاد، ظهرت مؤخّرًا الكثير من الشركات لتتخصص في بناء عتادٍ يحترم خصوصية المستخدم بصورة افتراضية. يكون سعر هذا العتاد عادةً مرتفع الثمن موازنةً بغيره، لكن إن كنتَ مهتمًا حقًا بتأمين نفسك إلى أقصى صورة ممكنة فحينها قد تحب الشراء من أحدها. هنا نذكر بعضها:

- Purism: شركة تبيع أجهزة حواسيب وهواتف محمولة، ليست مفتوحة المصدر (من ناحية تصميم العتاد) لكنها تستعمل تعريفات عتاد مفتوحة المصدر 100%. من مزاياها أنّ أجهزتها تأتي بقواطع فيزيائية (Kill Switches) للشبكة اللاسلكية والميكروفون والكاميرا المرفقين مع الجهاز، وهو ما يعني أنّك قادرٌ على فصل الكهرباء فيزيائيًا عن هذه المكوّنات لوحدها دونًا عن بقية المكونات. وإذا فصلتَ الكهرباء عنها، فمن المستحيل أن تقوم أي برمجية بتشغيلها ومحاولة المرور عبر أنظمة حماية البرمجيات للتجسس عليك. تدعم هواتفها المحمولة تغيير نظام التشغيل بالكامل بل وهي توزيعة من توزيعات لينكس في الواقع.
- Pine64: شركة تصنع الكثير من منتجات العتاد المختلفة (حواسيب محمولة، هواتف، دارات إلكترونية، أجهزة لوحية ...إلخ). لديها هاتف يعرف باسم PinePhone وهو هاتفٌ يأتي بتوزيعة لينكس افتراضيًا عليه.
- System76: شركة أمريكية تصنع حواسيبَ مكتبية ومحمولة تأتي بنظام لينكس مسبقًا، وتستعمل نظام إقلاع مفتوح المصدر لحواسيبها. ميّزة حواسيبها أنّها تعطّل افتراضيًا الكثير

من خواصّ التعقّب في العتاد مثل Intel ME وAMD Secure Technology. وهذه الخواص هي قِطع عتاد وبرمجيات موجود داخل المعالجات، وتسمح لها بإرسال البيانات إلى الشركة المطوّرة عن بُعد (حتّى والحاسوب مُطفئ!).

4.4. اختيار نظام التشغيل

يستعمل معظم القرّاء غالبًا نظام التشغيل ويندوز (Windows) من شركة مايكروسوفت (Microsoft) على أجهزة حواسيبهم، لكن هذا ليس أفضل خيارٍ موجود في الساحة من أجل الأمان الرقمي والخصوصية.

عليك بدايةً أن تعلم أنّه يمكنك حذف نظام التشغيل الحالي على أجهزة حواسيبك وتثبيت أيّ نظامٍ بديلٍ تريده. لدى مختلف أنظمة التشغيل مميزات وعيوب مختلفة وتطورها شركات ومؤسسات مختلفة حول العالم. ويندوز مثلًا يُطَوّر من طرف شركة مايكروسوفت وحدها، وكذلك ماك من طرف شركة آبل، أمّا نظام لينكس فهو يأتي على شكل توزيعات (Distributions) يطورها أفرادٌ وشركات مختلفة من حول العالم. هناك الكثير من أنظمة التشغيل الأخرى وليست هذه فقط الموجودة بالساحة، لكن هذه هي أشهرها ولا ننصح باستخدام غيرها.

إننا ننصح باستخدام أحد توزيعات نظام لينكس عوضًا عن ذلك، وهذا للأسباب التالية:

- توزيعات لينكس مفتوحة المصدر، وهو ما يعني أنّ الجميع قادرٌ على رؤية شِفرة البرامج المصدرية التي تأتي محمّلةً معها لضمان خلوها من برمجيات التجسس والبرمجيات الخبيثة. هناك الآلاف من توزيعات لينكس بالطبع وليس هناك ضمانٌ أنّ جميعها تأتي ببرمجيات مفتوحة خالية من الأبواب الخلفية، لكن معظمها هي كذلك في الواقع خصوصًا الشهير منها.
- تقريبًا كل توزيعات لينكس مجانية. وهو ما سيخلّصك كمستخدم من وجع الرأس المتعلق بتراخيص مايكروسوفت وبرمجياتها.
- لا تعمل الفيروسات على توزيعات لينكس (هناك عددٌ محدود جدًا من الفيروسات التي قد تصيب لينكس لسطح المكتب، هذا إن كانت موجودة أصلًا).
- التحديثات مستمرة دومًا على توزيعات لينكس ومجانية طوال الوقت، وهو ما يعني أنّه بإمكانك الترقية من إصدارٍ معين لتوزيعة لينكس إلى الإصدار الآخر وقت نزوله. تحديثات البرمجيات مستمرة طوال الوقت وهي في الغالب أسرع من ويندوز.
- لا تأتي توزيعات لينكس ببرمجيات تعقّب وإرسال بيانات كما في ويندوز، بل تقريبًا لا

يوجد أي اتصال بينك وبين خواديم مطوري التوزيعة سوى عندما تقوم بتثبيت برنامجٍ ما أو تنزيل التحديثات.

- يمكنك تفعيل وتعطيل أي برمجية أو خاصّيّة في لينكس، على عكس ويندوز. نظامك بالكامل تحت سيطرتك. لا يوجد أي صناديق سوداء على نظامك؛ لا يوجد برمجية لا يمكنك التحكّم بها أو الوصول إليها أو تقييدها أو تغيير طريقة عملها. كلّ شيء مفتوحٌ أمامك ومعروف.
- يجبرك لينكس على الخروج من منطقة الراحة لتعلّم العديد من أساسيات علوم الحاسوب وطريقة عمل الأنظمة، وهو ما سيرفع نسبة الوعي لديك مع الزمن خصوصًا إن كنت داخلًا على مجال علوم الحاسوب والبرمجة فستتطرق أولًا وآخرًا إلى لينكس.

هناك الآلاف من توزيعات لينكس التي تتخصص في مجالاتٍ معيّنة دونًا عن غيرها، إليك توزيعات لينكس التي نستحسنها بالإضافة إلى معلوماتٍ عنها:

1. أوبونتو: أشهر توزيعة لينكس على الإطلاق وقد بدأ تطويرها في 2004م. أوبونتو مبنية على توزيعة دبيان وتستعمل نظام التحزيم dpkg (بصيغة DEB.) وبرنامج إدارة الحزم apt. تعتبر من أفضل التوزيعات ليبدأ المستخدمون الجدد رحلتهم في عالم لينكس. هناك إصدارات قصيرة الدعم بالتحديثات (9 أشهر فقط) تُطلَق كلّ 6 أشهر وإصدارات طويلة الدعم (5 سنوات من التحديثات) تُطلق كل سنتين (مثل أوبونتو 16.04، ثم 18.04، ثم 20.04 ...إلخ). الإصدار الأخير وقت كتابة هذا الكتاب هو 20.04 وهو مدعوم إلى 2025م.

2. لينكس منت: توزيعة مبنية على أوبونتو، تستفيد من مميزاتها ولكن تأتي كذلك ببرامج ومميزات إضافية لتسهيل عمل المستخدم، مثل برامج خاصّة لإدارة البرمجيات والتحديثات والنُسَخ الاحتياطية وإدارة العتاد وأكثر من ذلك. ينصح بها بشدّة للمبتدئين.

هناك توزيعات أخرى بالطبع مثل فيدورا، أوبن سوزا، أرتش لينكس وغيرها. لكننا لا نستحسن البدء معها لكونها تتطلب خبرةً أكثر في استخدام نظام لينكس.

ستحتاج تعلّم العديد من المعلومات عن نظام لينكس قبل الانتقال إليه؛ مثلًا عليك أن تعلم أنّ برمجيات ويندوز (كل شيء بصيغة exe.) لا تعمل على لينكس، وبالتالي عليك البحث عن بدائل لتلك البرمجيات. يمكنك تثبيت نظام لينكس على نفس القرص الصلب بجانب ويندوز لتجرّبه إن أردت قبل الانتقال إليه بصورة كاملة. ننصحك بزيارة قسم لينكس على أكاديمية حسّوب وتصفّح المقالات المكتوبة هناك للمزيد من المعلومات عن لينكس.

كلّ ما سبق مفيدٌ إن قررت الانتقال إلى نظام لينكس. لكننا ندرك أنّ الكثير من القرّاء لن يقدروا على هذا التحوّل أو يريدوه، وبالتالي هناك بعض النقاط لأخذها بعين الحسبان إن قررت البقاء على استخدام ويندوز:

- ننصح دومًا باستخدام آخر إصدارات ويندوز، مثل ويندوز 10. لا تستعمل شيئًا مثل ويندوز 7 فقد انتهى دعمه بالتحديثات وصار مليئًا بالمشاكل والثغرات الأمنية التي لن تُرسل مايكروسوفت ترقيعاتِ (Patches) لإصلاحها. من الخطير أن تتصفّح الإنترنت بأحد أنظمة ويندوز التي انتهت فترة دعمها.
- احرص دومًا على الحصول على النسخ الأصلية من ويندوز كما ذكرنا في فصولٍ سابقة، ولا تستعمل برنامج قرصنة الحماية (Crack) لتحصل عليه. قد تكون تلك البرامج تتجسس عليك وعلى بياناتك الحساسة ولا تدري متى تنفجر لتحذف بياناتك مثلًا أو تسرق معلومات بطاقاتك الائتمانية. قد تستعملها لسنواتٍ دون أن تحصل مشكلة ثمّ فجأة يتم تفعيلها عن بُعد من طرف المُخترقِين لسرقة كامل بياناتك أو تشفيرها أو تدميرها. لا تخاطر ببياناتك وملفّاتك ومستقبلك فقط لتتجنب دفع القليل من المال لقاء برمجياتٍ تستخدمها كلّ يوم للوصول إلى العالم الرقمي والعمل فيه.
- لا تستعمل نظام التشغيل الأصلي الذي جاء مع الجهاز، بل احذفه تمامًا وثبّت نسخة جديدة بنفسك. لا يمكنك معرفة ما البرمجيات المُرفقة مع هذا النظام وبالتالي هناك احتمالية أن يحوي برمجيات مراقبة أو تعقّب من طرف الشركة المصنّعة أو الشركة التي تبيعك الجهاز. الحلّ الأفضل هو أن تحذفه ثمّ تثبّت واحدًا جديدًا، وإن كان جهازك يأتي بنسخة أصلية من ويندوز فيمكنك حينها تفعيل النظام الجديد بنفس مفتاح التفعيل (Activation Key) القادم مع الجهاز (يمكنك أن تسأل الجهة التي باعتك الجهاز لتحصل عليه إن لم تجده على علبة الحاسوب أو الوثائق المرفقة معه).

بخصوص نظام ماك (macOSe من شركة آبل هو نظامٌ يأتي افتراضيًا على أجهزة الشركة فقط ولا يأتي مع أجهزة شركاتٍ أخرى، فنسبة استخدامه ضئيلة بسبب ذلك. وهو مبنيٌ على يونكس (Unix) ومغلق المصدر. تمتلك شركة آبل تحكّمًا كاملًا به وكذلك ببيانات المستخدمين وحساباتهم فخدمات آبل المختلفة مدمجة فيه بصورة جذرية.

لا ننصح بشراء منتجات آبل ولا استخدام أنظمتها، فهي مغلقة المصدر وتمنع المستخدم من التحكّم بأجهزته وتثبيت ما يشاء عليها. لكنّها جيّدة من ناحية حماية المستخدمين من الأطراف

الثالثة (3rd-party)، حيث تدعم خدمات التشفير وتستخدمها بكثرة في منتجاتها، كما أنّها لا تبيع البيانات للمعلنين وتمتلك سياسات خصوصية واضحة تخبر المستخدم كيفية التعامل مع بياناته. وهي أفضل من مايكروسوفت في هذا المجال، وهذا لا يعني أنّ ويندوز لا يمكن ضبطه ليكون آمنًا من هذه الناحية كذلك، لكنّ الإعدادات الافتراضية هي ما يهمّ.

يُمكن تأمين كلّ الأنظمة بصورة قويّة من ناحية المبدأ، لكن ما يهم هو طريقة تعاملها مع بيانات وملفّات المستخدم وهل تأتي بإعدادات حفظ الخصوصية مفعلةً افتراضيًا أم لا، وهل تجبره على نوعٍ معيّن من الممارسات بعقله اللاواعي أم تجعله مدركًا لِمَا يحصل على نظام تشغيله. لا يمكن الحكم على نظام تشغيل معيّن أنّه أأمن نظام تشغيل على الإطلاق مثلًا، لكن هناك أنظمة يمكن تأمينها بسهولة أكثر من غيرها وهناك أنظمة مفتوحة وأخرى مغلقة، ومنها ما يحترم الخصوصية وحقّ المستخدم في التصرّف بعتاده ومنها ما لا يحترم ذلك.

فمثلًا حتّى لو استخدمت خدمات التشفير بصورة جيدة من شركة آبل على نظام macOS واستخدمت خيارات الحماية الأساسية، فسيظل عرضةً للاختراق إمّا عبر الثغرات الأمنية الغير مكتشفة بعد أو البرمجيات الخبيثة التي قد تصل حاسوبك بطريقةً ما. لا يوجد نظام مؤمَّن مئة بالمئة.

4. 5. اختيار متصفح الويب

أفضل متصفّح ويب يجمع بين احترام الخصوصية والأداء وسهولة الاستخدام هو فيرفكس (Firefox). ننصح ألّا يستعمل المستخدمون متصفّح كروم (Google Chrome) من شركة جوجل إن كانوا مهتمين حقًا بخصوصيتهم.

متصفّح كروم من جوجل مغلق المصدر (هو في الواقع مبني على متصفّح كروميوم (Chromium) المفتوح المصدر التابع لجوجل كذلك، لكنّ كروم نفسه مغلق المصدر) وبالتالي لا أحد يعلم ما الموجود داخله سوى مطوروه. لكن هذه ليست ربع المشكلة ولا حتّى ثُمنها، بل المشكلة الحقيقية هي في البيانات والأساليب التي يتّبعها كروم افتراضيًا [1]:

- يسجل كروم دخولك إلى حسابك عبر ميّزة موجودة داخل المتصفّح مباشرةً عندما تسجِّل الدخول إلى أحد مواقع خدمات جوجل. وهو ما يعني أنّ كل بياناتك والمواقع التي تزورها وكل أنشطتك على الشبكة صارت لدى جوجل لأنّ حسابك صار مربوطًا بمتصفّح الويب نفسه. حتّى عند تعطيل الميزة تبقى صفحة البداية تقوم بتسجيل دخولك تلقائيًا إلى حسابك على جوجل.

- لا يمنع كروم أي نوعٍ من أنواع شِفرات التعقّب والإعلانات (Tracking & Ads Scripts) افتراضيًا، وهو ما يعني أنّ كل المواقع التي تزورها قادرة على معرفة كل شيء عنك.
- يُرسل كروم (على الهواتف المحمولة) البيانات التالية تلقائيًا إلى خواديم جوجل: أقرب موّجهات الشبكة اللاسلكية (Routers) إليك، ومعرّفات أبراج الاتصالات الخلوية الأقرب إليك (Cell Tower IDs)، وقوّة شبكتك اللاسلكية الحالية. وإذا سمحت لأحد مواقع الويب بالوصول إلى بيانات موقعك الحالية (Location Data)، فحينها ستُرسل هذه البيانات إلى تلك المواقع كذلك.
- يتصل كروم دوريًا بخواديم جوجل للتحقق من وجود تحديثات، وهو ما يُرسل عنوان الآي بي الخاص بك بصورة يومية إلى خواديمهم. يسمح لهم هذا بمعرفة عدد المستخدمين في كل دولة حول العالم. وإن كان هذا الأمر موجودًا على المتصفّحات الأخرى إلّا أنه يمكن تعطيله فيها، على عكس كروم (إلّا بطريقة صعبة على معظم المستخدمين).
- إذا سجّلت الدخول إلى حسابك في جوجل فكل عمليات البحث التي أجريتها سابقًا موجودة ومحفوظة هناك افتراضيًا.
- يُرسل كروم كل عناوين الويب التي تزورها إلى جوجل من أجل توفير ميّزة الاقتراحات (Suggested Pages). لكن يمكنك تعطيل الميزة من إعدادات كروم إن أردت.
- يُرسل كروم بياناتٍ محدودة ومجهولة الهوية على حد وصفه عن مربّعات الإدخال (Web Forms) التي تصادفها على مختلف مواقع الويب، وهي المربّعات التي تدخل فيها اسم المستخدم وكلمة المرور مثلًا، ويريد كروم أن يعرف هيكلة هذه المربّعات وطريقة تعاملك معها.
- يحلل كروم اللغة الافتراضية لمعظم مواقع الويب التي تزورها لكي يعرف ما هي لغتك الافتراضية التي تحبّ التصفّح بها، ثم يعرض عليك ترجمة أي محتوى لا يكون بتلك اللغة. يقوم كروم بإرسال هذه المعلومة إلى خواديم جوجل كذلك.
- إذا تركت خيار "إرسال البيانات إلى جوجل" فعّالًا، فسيقوم المتصفّح بإرسال الكثير من البيانات عنك وعن مواقع الويب التي تزورها وطريقة تفاعلك معها والنقرات التي تنقرها إلى خواديم جوجل.
- عند تثبيت كروم على ويندوز، يقوم المتصفّح بإرسال معرّف فريد (Unique ID) عن جهازك إلى خواديم جوجل لأوّل مرّة لإحصاء عدد التثبيتات. وهو ما يعني نظريًا قدرتهم على ربط

عنوان الآي بي الخاص بك بكل بياناتك الحسّاسة الأخرى السابق ذكرها والتي سيأتي ذكرها.

- قد تقوم جوجل بإجراء بعض التجارب على بعض مستخدمي كروم، ويمكنها فعل ذلك عبر استهدافك عبر عنوان الآي بي الخاص بك أو نظام التشغيل أو إصدار المتصفّح الذي تستعمله، وهو ما يعني أنّ هذه البيانات متوفرة لديهم.
- استخدامك لأي ميزة إضافية داخل المتصفّح يعرّضك لانتهاكات خصوصية أكبر؛ ميزة البحث الصوتي مثلًا تجعل جوجل تسجّل كل ما تقوله داخل الغرفة حتّى عند عدم عمل الميزة في نفس الوقت. ميّزة المزامنة والإكمال التلقائي والتدقيق الإملائي تجعل المتصفّح يرسل كل حرف تكبسه على لوحة مفاتيحك إلى خوادم الشركة.

ننصح من أجل كلّ هذه الأسباب باستخدام فيرفكس:

- هو متصفّح مفتوح المصدر بالكامل ويمكن للجميع رؤية شِفرته البرمجية.
- موزيلا، الشركة التي تقف خلفه مهتمة جدًا بالخصوصية ومكافحة انتهاكاتها على الشبكة، ولها باعٌ طويلٌ في هذا المجال.
- يمتلك المتصفّح ميزة تمنع سِكربتات التعقب والإعلانات السيئة من العمل بصورة افتراضية، وهو ما يحمي خصوصيتك.
- يمنع المتصفّح ملفّات تعريف الارتباط للطرف الثالث (3rd-party Cookies)، وهو ما يعني أنّ مواقع الويب التي تزورها لا يمكنها معرفة النشاطات التي قمت بها على مواقع الويب الأخرى، بل فقط مواقعها هيَ نفسها.
- يمنع المتصفّح ملفّات تعريف الارتباط التي تعمل على أكثر من موقع. فمثلًا إذا قمت بتسجيل الدخول إلى فيس بوك ثمّ فتحت أي موقع محتوى آخر به بعض أزرار المشاركة التابعة لفيس بوك، فيمكن لفيس بوك أن يتعقّبك عبر هذا. يقوم فيرفكس بمنع هذا الأمر افتراضيًا.
- يمنع المتصفّح تعقّب المستخدمين عبر بصمة الإصبع (Fingerprint) الخاصّة بالمستخدم، وهي المعلومات حوله وحول متصفّحه ونظامه التي تسمح لأصحاب مواقع الإنترنت بتمييز المُستخدم من بين المستخدمين الآخرين
- لا يوجد تسجيل دخول تلقائي داخل المتصفّح إلّا إن قمت به بنفسك، وحسابك على فيرفكس مفصولٌ عن مواقع الويب التي تزورها.

- لا يرسل المتصفّح بياناتٍ عنك أو عن مواقع الويب التي تزورها، أو نشاطاتك أو نقراتك إلى الشركة. وسياسة إرسال البيانات الافتراضية محدودة أكثر بكثير من سياسة جوجل. ما يزال المتصفّح يُرسل عنوان الآي بي الخاص بك إلى موزيلا عند التثبيت لأوّل مرة مع ذلك.

هناك متصفّحات أخرى توفّر خصوصية أكبر من فيرفكس كذلك، مثل Ungoogled Chromium (وهو متصفّح كروم لكن دون خدمات جوجل تمامًا) وننصح به لمن يريد نفس أداء كروم لكن بخصوصية أكبر.

إذا كنت تريد متصفحًا مفتوح المصدر وبنفس واجهة ومميزات كروم (بل حتّى نفس المحرّك) ويتمتع بالخصوصية والأمان بنفس الوقت فيمكنك تجريب متصفّح Brave، وهو متصفّح مبني على كروميوم مع إعدادات خصوصية قوية افتراضيًا بالإضافة إلى بعض التقنيات المتطورة لدعم صنّاع المحتوى والمواقع التي تزورها عبر العملات الرقمية وغير ذلك. يحميك Brave حتّى من تتبع بصمة الإصبع افتراضيًا.

6.4. البدائل مفتوحة المصدر للبرمجيات الشهيرة

إليك جدولًا مفيدًا بالبرمجيات الشهيرة مغلقة المصدر، وما يقابلها من معسكر البرمجيات المفتوحة. يمكنك زيارة مواقع هذه البرمجيات وتحميلها وتثبيتها على جهازك لرؤية ما إذا كانت تناسب استعمالك اليومي أم لا.

البدائل المفتوحة	البرامج المغلقة	اسم التصنيف
LibreOffice: طقم مكتبي مجاني ومفتوح المصدر. نشأ من اشتقاق (Fork) من برنامج OpenOffice قبل نحو عشر سنوات. يمتلك دعمًا جيّدًا لفتح وتصدير ملفّات مايكروسوفت أوفيس. OnlyOffice: طقم مكتبي مفتوح المصدر يأتي بواجهة شبيهة بمايكروسوفت أوفيس. يدعم فتح أكثر من مستند داخل تبويبات في نفس النافذة تمامًا كمتصفّح ويب.	مايكروسوفت أوفيس	برامج المكتب

البدائل المفتوحة	البرامج المغلقة	اسم التصنيف
GIMP: برنامج لتحرير وتصميم ومعالجة الصور. يُعتبر من أفضل البدائل المفتوحة للفوتوشوب. Krita: برنامج رسم يأتي بعددٍ من المميزات المتقدّمة، يدعم الرسوم المتحرّكة ثنائية الأبعاد (2D) عبر إضافات خارجية. Inkscape: بديل للإليستريتور من شركة أدوبي للرسم المتجهي (Vector).	Adobe Photoshop CorelDraw Adobe Illustrator	برامج التصميم والرسم
Blender: البديل المفتوح الوحيد بنفس مستوى الجودة لبرامج التصميم المغلقة ثلاثية الأبعاد. تستعمله الكثير من الشركات لتصميم الرسوم المتحرّكة الخاصّة بها للأفلام والألعاب.	Maya Cinema 4D Lightwave 3D SolidWorks	برامج التصميم ثلاثية الأبعاد
FreeCAD: يدعم النمذجة ثنائية وثلاثية الأبعاد والاستيراد والتصدير من صِيغ الملفّات المعيارية الشهيرة في المجال. LibreCAD: للنمذجة ثنائية الأبعاد فقط. واجهته أبسط وأسهل للاستعمال.	AutoCAD	برامج النمذجة
TestDisk: أداة سطر أوامر لاسترجاع البيانات والملفّات المحذوفة على مختلف أنظمة التشغيل (ويندوز، ماك، لينكس). PhotoRec: برنامج مُرافِق لـTestDisk يركّز على استرجاع ملفّات الملتيميديا من مختلف وسائط التخزين كبطاقات الذاكرة وفلاشات USB وغيرها.	-	استعادة البيانات
VLC: من أشهر برامج تشغيل الوسائط المتعددة بمختلف الصِيغ، ولا يعرف الكثير من الناس أنّه مفتوح المصدر في الواقع ومجاني تمامًا.	Windows Media Player PowerDVD	تشغيل الوسائط

البدائل المفتوحة	البرامج المغلقة	اسم التصنيف
TigerVNC: موجود من 1999م ويركّز على عامل الأداء لإمكانية تشغيل الألعاب والوسائط عن بُعد بين الأجهزة المختلفة عبر الشبكة. FreeRDP: للوصول إلى أجهزة ويندوز عن بعد عبر بروتوكول RDP من مايكروسوفت. Apache Guacamole: على عكس بقية البرامج فهو ليس برنامجًا ليُثبّت على النظام، بل يُثبّت فقط على جهاز سطح المكتب البعيد كخادوم (Server) ثمّ يُمكن فتحه من داخل متصفّح الويب مباشرةً.	TeamViewer	الوصول البعيد (Remote Desktop)
Jitsi: يدعم حتّى 75 شخصًا في نفس الاجتماع، ويدعم تشفير طرف-لطرف (End-to-End Encryption) بالإضافة للمحادثة الصوتية والمرئية ومشاركة الشاشة والملفّات بين المستخدمين. BigBlueButton: مناسب للمنشآت التعليمية أكثر حيث يمتلك حزمة من الامتدادات لجعله يتكامل مع ووردبريس وMoodle وغيرها من سكربتات إدارة المحتوى. يدعم نحو 100 مستخدم في نفس الجلسة	Zoom Skype	برامج الاجتماعات

4. 7. التحديثات وسياسة التحديث

التحديثات مهمّة جدًا لأي مستخدم مهتم بالأمان الرقمي والخصوصية. تأتي تحديثات البرمجيات عادةً لإصلاح المشاكل الأمنية أو تقديم مميزاتٍ جديدة، وعدم تثبيت المستخدم لها على حاسوبه سيجعله عرضةً للثغرات الأمنية.

حوالي 75% من كل الثغرات التي يستخدمها المخترقون حول العالم (إحصائيات الربع الأول من 2020م) كانت ثغراتٍ متعلّقة بحزمة مايكروسوفت أوفيس مثلًا [1]. تسمح هذه الثغرات للمخترقين بوضع شِفرات خبيثة داخل ملفّات المستندات وإرسالها إلى المستخدمين المُراد اختراقهم، والذين يفتحونها للأسف دون وعي مما يسمح للمخترقين بالتحكّم بكامل أنظمتهم أو سرقة بياناتٍ حساسة لهم.

والأمر لا يقتصر على رسائل التصيّد (Phishing) التي تأتي من المخترقين بصورة مباشرة، بل

يمكن مثلًا أن يقوم أحد المخترقين باختراق حساب صديقك أو زميلك في العمل مثلًا، ثم يُرسل لك أحد هذه الملفّات وتظن أنت أنّه لا بأس بفتحه فهو قادمٌ من صديقك، فتُخترَق أنت كذلك عبر هذه الطريقة.

عليك الحفاظ على نظامك مُحدّثًا دومًا من أجل هذا، وسواءً كنت تستخدم ويندوز أو ماك أو لينكس. تأكّد كل أسبوع على الأقل أنّ نظامك وبرمجياتك جميعها محدّثةٌ إلى آخر إصدارٍ منها، وخصوصًا متصفّحات الويب، فمتصفّحات الويب هي بوابتك الأساسية للحصول على البيانات من الجهات الأخرى واستعمالك لمتصفّح ويب قديم سيعرّضك للاختراق.

ولكن المستخدمين لا يستمعون إلينا للأسف. فعلى سبيل المثال كانت أحد الثغرات التي أُصلِحت في مايكروسوفت أوفيس سنة 2017م ما تزال هي واحدة من أكثر 10 ثغرات استخدامًا لاختراق الناس في 2020م [2]، وهو ما يعني أنّ المستخدمين لا يقومون بتحديث برمجياتهم بالصورة المطلوبة.

لا تكن مثلهم!

4. 8. ختام الفصل

لا تكن مثل هؤلاء المستخدمين الذين لا يبالون بنوعية البرمجيات التي يثبّتونها على أنظمتهم ولا يهتمون بتحديثها. قد تشكّل كل هذه العوامل خطرًا عليك في المستقبل إن لم تضبطها بصورةٍ صحيحة. وضبطها ليس بذاك التعقيد فكلّ ما عليك فعله هو اختيار البرمجيات الجيّدة بدايةً، ثمّ متابعة تحديثها بصورة مستمرة، فقط هذا هو كلّ الأمر.

5. اختيار الخدمات والمزودات

سنشرح في هذا الفصل كيف تختار أفضل المزوّدات الإلكترونية التي تعرض عليك أهمّ الخدمات التي أنت بحاجة لاستعمالها، مثل خدمات البريد والبحث والمحادثة وغير ذلك.

سنشرح أوّلًا المبدأ العام لكيفية اختيار هذه الخدمات بحيث تكون قادرًا على اتخاذ القرار بنفسك، ثم سنقدّم لك مجموعة من الخدمات المُقترحة.

5. 1. مَلَكة اختيار الخدمات

هناك الكثير من موفّري الخدمات المختلفة التي قد تحتاج إليها على الإنترنت، لكن كيف تختار التي تحفظ الخصوصية والأمان الرقمي منها بأفضل صورة ممكنة؟ وما هي المعايير لهذا الاختيار؟

الإجابة على هذا السؤال فرعٌ عن إجابتك عن سؤال إلى أي درجة تريد حماية نفسك؟ الذي قدمّناه في فصلٍ سابق. عليك أن تحدد من تريد حماية نفسك ضده وإلى أي مدى أنت مستعد أن تصرف الوقت والمال والجهد في سبيل ذلك.

دعنا نبدأ الحديث عن موضوع أماكن عمل هذه الخدمات. كل الشركات التي تعرض عليك خدمات البريد الإلكتروني والبحث والمحادثة ...إلخ. يكون لها مقرّ رئيسي خاضع لسيطرة دولة معيّنة، وهي بالتالي تخضع لقوانين تلك الدولة. فإذا كانت الشركة مركزها في أمريكا مثلًا فهي تخضع للقوانين الأمريكية. وهذا عاملٌ مهم لتضعه في عين الاعتبار عندما تختار الخدمات الإلكترونية التي تريد استعمالها.

هناك قوانين أمنية كثيرة قد تُجبر الشركات على تسليم مفاتيح التشفير (Encryption Keys)

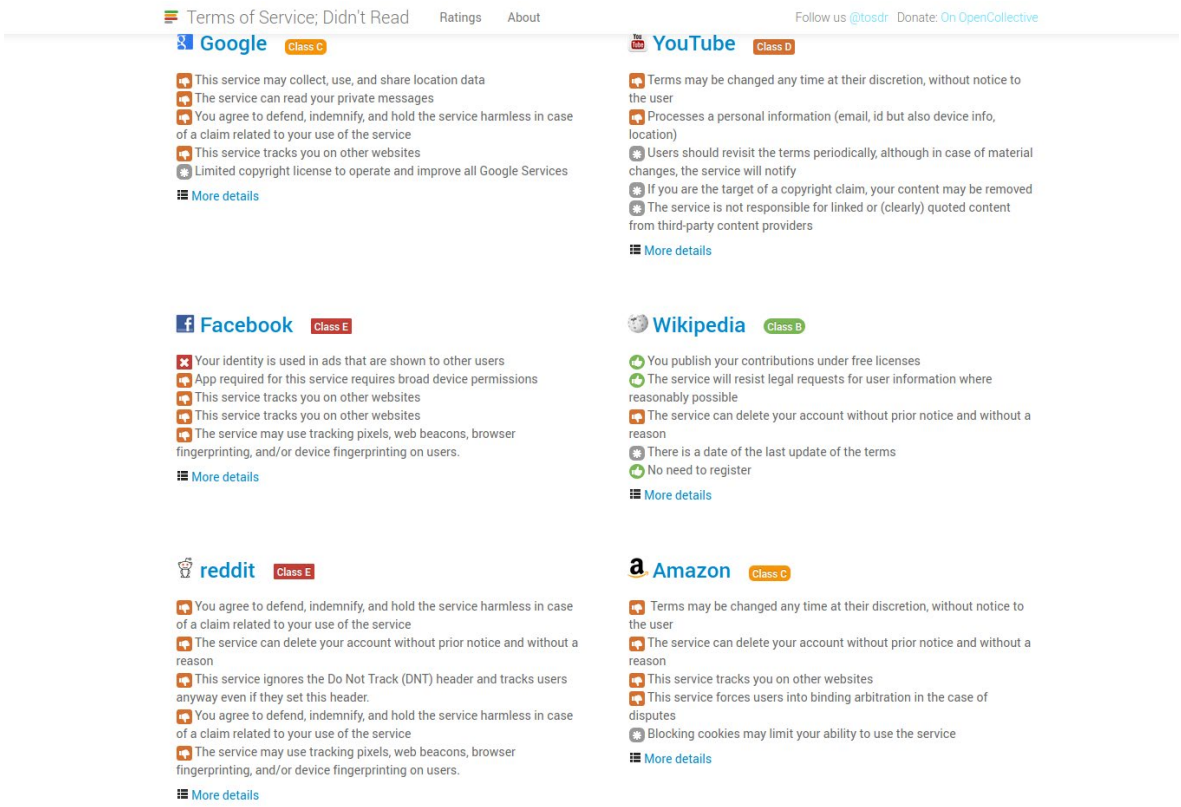
للسلطات عند طلبها من القضاء. تُستعمل مفاتيح التشفير لتشفير البيانات المهمّة لدى هذه الشركات وتسليمها يعني أنّ الشركات العاملة في هذه الدول عرضة للمراقبة وكشف كل اتصالات ومعلومات مستخدميها في أي وقتٍ تريده حكومات هذه الدول. إليك قائمة بها:

- الدول التي تفرض تسليم مفاتيح التشفير بأمر من القضاء: أنتيجويا وباربودا، وأستراليا، وكندا، وفرنسا، والهند، وإيرلندا، والنرويج، وروسيا، وجنوب إفريقيا، والمملكة المتحدة.
- الدول التي قد تطلبها عند الحاجة: بلجيكا، وإستونيا، وفنلندا، ونيوزيلندا، وهولندا، والولايات المتحدة الأمريكية.
- الدول التي لا يوجد بها قانون لذلك: جمهورية التشيك، وألمانيا، وأيسلندا، وإيطاليا، وبولندا، والسويد، وسويسرا.

تعد سويسرا من أفضل البلدان في تشريع قوانين الحماية والخصوصية؛ فهي تمتلك حزمةً من القوانين المتعلقة بحماية خصوصية الأفراد، وهي أفضل من غيرها في هذا المجال، لكن هذا لا يعني أنّها لا يوجد بها قوانين تُجبر الشركات على تسليم البيانات؛ فإذا طلبت المحكمة السويسرية من شركةٍ ما على أراضيها تسليم بيانات معيّنة عن مستخدمٍ ما، فحينها على الشركة الالتزام بذلك [3]، والفرق الوحيد مع الولايات المتحدة في هذا المجال هو أنّها مطالبةٌ كذلك بإبلاغ المُستخدم عن هذه العملية في نفس الوقت ليعلم أنّه تتم مراقبته.

نأتي الآن إلى شروط الاستخدام وسياسات الخصوصية الخاصّة بموفّري الخدمات الإلكترونية أنفسها. كل الشركات تعرض عليك هذه الشروط قبل تسجيلك بحسابٍ لديها، وأنت مطالبٌ بالموافقة قبل أن تنضم إليها. وللأسف الشديد لا يقرأ الناس هذه الشروط فيوافقون عليها دون أن يدروا بالموجود فيها.

يمكنك استخدام خدمة "Terms of Service: Didn't Read" لحل هذه المشكلة، حيث تعرض لك في نقاطٍ سريعة أبرز الشروط المتعلّقة بأشهر مزوّدي الخدمات مثل فيس بوك وتويتر وأمازون ويوتيوب وغيرهم. وهكذا تعرف ما هي الاشتراطات التي تشترطها عليك هذه الخدمات دون الحاجة إلى قراءة كامل شروط الاستخدام الطويلة الخاصّة بها.



صرت تعرف الآن ما يترتب عليك عند الاشتراك في خدمة جديدة. لكن ماذا إن كانت شروط الاستخدام لخدمة معينة لا تعجبك، أو لا تريد استخدام خدمات الشركات الأمريكية - وهي الأكثر شيوعًا - ؟ حينها عليك البحث عن بدائل.

قام الكثير من الناس المهتمين بالخصوصية بالفعل بإنشاء الكثير من الأدلّة على الشبكة للبدائل الأكثر احترامًا للخصوصية من غيرها. من بينها موقع Privacy Tools، حيث تجد على موقعهم قوائم طويلة بالخدمات المَنصوح استخدامُها بالإضافة لملاحظات عديدة حولها.

لاحظ أنّه لا يمكنك ضمان أمان وخصوصية هذه الخدمات، حتّى لو كانت الشفرة المصدرية للخدمة مفتوحة المصدر بالكامل، وهذا لأنّك لا تضمن أنّ نفس الشفرة المصدرية التي تراها أنت هي نفسها التي تعمل على خواديم تلك الشركة في الواقع دون أي تغيير أو تعديل. الثقة هي كل شيء هنا.

سنقدّم بعض هذه الخدمات. ونرجو من القارئ أن يستوعب أنّ استحساننا لها هنا لا يعني موافقتنا عليها في كل شيء ولا أنّها ستكون آمنة دومًا؛ فربّما تتغير طريقة عملها بعد بضع سنوات ونحن غير مسؤولين عن أي مشكلة معها بعد تاريخ نشر هذا الكتاب.

5. 2. اختيار خدمة البريد الإلكتروني

جميع خدمات البريد الإلكتروني متساوية في السوء من ناحية الوصول إلى بياناتك، فأنت لا تضمن في الواقع أنّ كل ما تقوله هذه الشركات عن أنّها آمنة وأنّها لا تشارك بياناتك مع أحد... إلخ هو أمرٌ صحيح ومطبّق في الواقع. لكن بعض الخدمات أفضل من بعضها، وننصح بتجنّب الخدمات الشهيرة مثل GMail وOutlook وغيرها إن أردت ألّا يطّلع أحدٌ على رسائلك الإلكترونية.

هناك ما يعرف بـ"التدقيق الأمني المستقل" (Independent Security Audit) وهي اختبارات أمنية تجريها فرق أمنية مستقلة متخصصة في الحماية والأمان لهذه الخدمات، حيث تجريها عبر الوصول إلى خواديمها وبياناتها الداخلية للتأكّد من مزاعم هذه الشركات. إذا كانت الخدمة التي تشترك بها لديها سجّل سابق بهذا النوع من الاختبارات فهذا أدعى للوثوق بها، لكن لا يمكنك بالطبع الوثوق بها 100% فقد تغير مثلًا من طريقة عملها بعد انتهاء التدقيق. لا يوجد شيء لتثق به 100% على الشبكة.

الشيء الثاني لتبحث عنه في خدمات البريد الإلكتروني هو التشفير؛ هناك ما يعرف باسم "تشفير طرف لطرف" (End-to-End Encryption) وهو طريقة تشفيرٍ تضمن أنّ صاحب الرسالة الأصلية والشخص الذي أُرسِلت إليه الرسالة فقط قادران على قراءتها دون أي جهة أخرى، بما في ذلك الشركة صاحبة الخدمة نفسها. ابحث عن الخدمات التي تستعمل هذا التشفير دومًا.

الشيء الأخير لتبحث عنه هو سياسة الشركة في الوصول إلى بياناتك وتسجيلها. هناك ما يعرف بسياسة "وصول صفر" (Zero-Access Policy) وهو ما يعني أنّ الشركة تلتزم بألّا يصل أحدٌ إلى أيّ بيانات عنّك من طرف موظّفيها إطلاقًا، إلّا في حال طلب من المحاكم أو الدول. وهناك كذلك ما يعرف بـ"سياسة صفر سجلّات" (Zero-Log Policy) وهو ما يعني أنّ الشركة لا تحتفظ بأي سجّلات عنك وعن طريقة استخدامك للخدمة.

الموقع	الوصف	الدولة	الخدمة
ProtonMail.com	خدمة بريد إلكتروني تستعمل تشفير End-to-End ولديها سياسة «وصول صفر» (Zero Access) لرسائل البريد الإلكتروني، مما يعني أنه حتى أصحاب الخدمة ليسوا قادرين على قراءة رسائل بريدك الإلكتروني (لكن ما يزال لديهم وصول إلى عناوين ومعلومات الرسائل، وعنوان الآي بي الخاص بك وبيانات عامّة عن حسابك مثل اسمك ومعلومات الدفع). توفّر اشتراك مجاني بسيط وبعدها سيتوجب عليك الدفع شهريًا للخدمة. ننصح بها بشدّة لولا أنه لديها بعض المشكلات في دعم اللغة العربية.	سويسرا	ProtonMail
TutaNota.com	توفّر تشفيرًا تامًا لكل بياناتك وحتى البيانات الفوقية للرسائل، ولا تقوم بتسجيل عنوان الآي بي الخاص بك إلّا بطلب من المحكمة الألمانية. لديها اشتراك مجاني محدود واشتراك مدفوع. ننصح بها.	ألمانيا	Tutanota

5. 3. اختيار محرك البحث الافتراضي

المستخدم في ناحية أضعف من ناحية محركات البحث، فلا شيء يوازي جوجل من ناحية السرعة وجودة النتائج. لكن يمكن أن تعجب البدائل الأخرى الكثير من المستخدمين كذلك.

الموقع	الوصف	الدولة	الخدمة
StartPage.com	محرك بحث شهير يوفّر لكن نفس نتائج جوجل، لكن دون وصلك بخواديمها، حيث يأخذ ما تبحث عنه ويرسله إلى جوجل ثم يعيد النتيجة إليك فقط دون إرسال عنوان الآي بي الخاص بك إليهم مثلًا (هو يعمل كوسيط بينك وبين جوجل). كان مقرّه في هولندا ولكن اشتُري مؤخرًا من شركة أمريكية.	هولندا ثمّ أمريكا	StartPage
DuckDuckGo.com	صحيحٌ أنّ مقرّه في أمريكا لكنّه يزعم أنّه لا يسجّل أي بيانات عنك ولا حتّى عنوان الآي بي الخاص بك عندما تقوم بعمليات البحث، بل يأخذ ما تبحث عنه ويسجّله بصورة مجهولة تمامًا دون ربطه بأي معلومات عنك أو عن متصفحك (وفق زعمه). بعض الروابط التي تزورها كروابط متجر أمازون قد تحوي على شِفرة تعقّب (Referral Code) خاص بالمحرّك لجعله يكسب بعض الأرباح، لكن DuckDuckGo يقول أنّه يستخدم هذه التقنية فقط مع المتاجر التي لا تسرّب بيانات المستخدمين إلى أطراف أخرى.	أمريكا	DuckDuckGo

5.4. خدمات المحادثة والتواصل

إليك الترشيحات التي اخترناها وقت كتابة هذا الكتاب:

الموقع	الوصف	الدولة	الخدمة
Signal.org	يعتبر من أكثر البرامج أمانًا وهو مفتوح المصدر بالكامل (بما في ذلك تطبيقات الواجهة (Clients) والخادوم). يستعمل تشفير End-to-End. حصل على تدقيق من فريق أمني مستقل للتأكّد من سلامته وأمانه	أمريكا	Signal
Telegram.org	واجهة التطبيقات (Clients) مفتوحة المصدر، لكن نسخة الخادوم مغلقة المصدر. تلجرام لا يستعمل تشفير End-to-End افتراضيًا لكنّه يدعم ذلك للمحادثات السرّية، كما يدعم تحديد مدة معيّنة للرسائل قبل أن تدمّر تلقائيًا بصورة ذاتية. ومن أجل الحماية والتخلص من طلبات الحكومات المختلفة لبيانات المستخدمين فقد بناه فريق التطوير بحيث تكون مفاتيح التشفير موزّعة على دول عدّة حول العالم وليس في دولة واحدة فقط، مما يعني أنّ على عدّة دول أن تقدّم نفس الطلب لكشف بيانات نفس المستخدم في نفس الوقت للتمكن من كشف هويته، وهو ما لم يحصل قطّ. أُسس تلجرام من قبل مليونير روسي معادي للحكومة الروسية.	دولي	Telegram
Wire.com	مفتوح المصدر (مع بعض القيود على نسخة الخادوم) ويستخدم تشفير End-to-End. مقرّه في سويسرا مما يجعله يتمتع بقوانين حماية وخصوصية جيدة. حصل على عدّة اختبارات تدقيق أمنية من فِرَق وجهات مختصة مختلفة. لكنّ استخدامه يتطلب اشتراكًا مدفوعًا، وهو مناسب أكثر للشركات.	سويسرا	Wire

5. 5. اختيار خدمة تخزين سحابي

اختيار خدمة التخزين السحابي موضوع أكثر صعوبة وهذا لأنّ المستخدم عادةً ما يحتاج أكثر من مجرّد تخزين ملفّات، بل يحتاج بعض المزايا الأخرى مثل المزامنة والمشاركة ...إلخ. والمشكلة هي أنّ التخزين السحابي مُكلف للشركات، فلن تجد من يقدمه لك مجانًا.

من أجل هذا ننصح باستخدام NextCloud وإنشاء نسختك الخاصّة على خادوم خاص بك. وNextcloud هو حزمة برمجيات سحابية لاستضافة الملفّات ومشاركتها بالإضافة لمزايا أخرى مثل التقويم والمحادثة والمجموعات وغيرها، شبيه جدًا بتطبيقات Google Docs, Google Drive وأمثالها من جوجل. قد تكون عملية إنشاء الخادوم معقّدة بعض الشيء ولهذا قد تحتاج توظيف أحد الخبراء على مواقع العمل الحرّ لينشئها لك إن لم تعرف عملها بنفسك. تتضمن حزمة Nextcloud دعمًا للكثير من البرمجيات الأخرى مثل LibreOffice Online، وهي نسخة من الحزمة المكتبية الشهيرة ليبر أوفيس البديلة لمايكروسوفت أوفيس لكن للاستخدام عبر الشبكة، حيث ستكون مثل Office 365؛ تعمل من داخل متصفّحك.

5. 6. اختيار الخدمات الأخرى

من أجل اختيار الخدمات الأخرى، ننصح بمراجعة موقع PrivacyTools.io أو AlternativeTo.com للبحث عن أفضل البدائل المتوفّرة للخدمات والمزوّدات الشهيرة.

إليك بعض النصائح العامّة لاختيار الخدمات مهما كان تصنيفها:

- ابتعد عن الشركات الأمريكية والشركات التي تتمركز في دول سيّئة السمعة من ناحية قوانين الخصوصية.
- ابحث دومًا عن الخدمات التي تدعم تشفير End-to-End، أو لديها سياسة صفر وصول (Zero-Acess Policy) وصفر سجلّات (Zero-Logs Policy).
- بخصوص البريد الإلكتروني فتجنّب إنشاء خادومك الخاص لاستضافة البريد الإلكتروني مهما كان السبب (إلّا إن كنتَ محترفًا في مجال الحماية والأمان الرقمي، وحينها لا تحتاج هذا الكتاب)، وهذا لأنّ تأمين البريد الإلكتروني وحلّ مشاكله والمحافظة على استمراريته على مدار السنين عملية شاقّة جدًا لا يقدر عليها معظم التقنيين بصورة جيدة. استخدام أي خدمة مثل GMail وOutlook سيكون أفضل من استخدامك لخدمة بريد إلكتروني خاصّة بك.

- ابحث عن الخدمات المفتوحة المصدر، والتي تنشر الشفرة المصدرية للبرمجيات التي تقدّمها، فهذا أدعى لتكون أكثر أمانًا وخالية من برمجيات التجسس والأبواب الخلفية.

5. 7. ختام الفصل

إذا كنتَ حقًا تبحث عن الخصوصية فحينها عليك الدفع لقائها. الخصوصية غالبًا لا تأتي مع الخدمات المجّانية لأنّك إن لم تدفع لقاء المنتج، فحينها بياناتك أنت هي المنتج. يعود قرار الخدمات التي تختارها أو تتجنبها إلى طبيعة الحماية والأمان اللذان ترغب بهما كما بيّنا في فصلٍ سابق.

6. تأمين الأشياء الأساسية المحيطة بك

سيشرح هذا الفصل طريقة تأمين بعض الأمور الأساسية المحيطة بك مثل نظام التشغيل للحواسيب وجهاز الموجّه (Router). كما سنشرح أهميّة استخدام بعض الأدوات والبرامج الإضافية لزيادة الأمان والحماية والخصوصية.

6. 1. تأمين أنظمة ويندوز

سيشرح هذا القسم أهمّ ما يجب عليك فعله لتأمين أنظمة ويندوز 10.

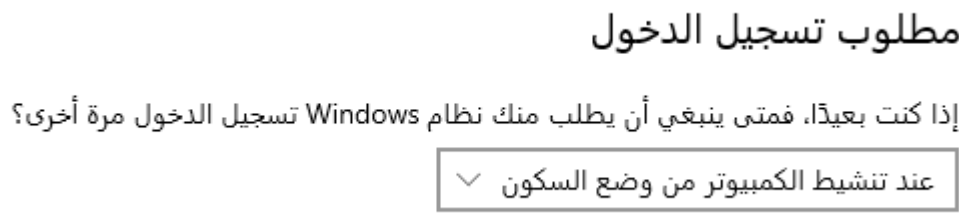
6. 1. 1. استعمال حساب محلي

تأكّد أنّ ما تستعمله للدخول إلى نظام ويندوز الخاصّ بك هو حساب مستخدم محلّي (Local User Account) وليس حسابًا من مايكروسوفت. وهذا لأنّ استخدامك للأخير سيعني ربط كل معلوماتك على حساب مايكروسوفت بكل الموجود على جهازك من بيانات وملفّات ونشاطات. يمكنك فعل ذلك عبر الذهاب إلى الإعدادات (Settings) --> الحسابات (Accounts) والتأكّد من نوع الحساب كما في الصورة:

6. 1. 2. استخدام كلمة مرور للدخول

من المهم جدًا أن تستعمل كلمة مرور للدخول إلى حاسوبك بدلًا من أن تجعله مفتوحًا بلا كلمة مرور، وهذا لحمايته من المتطفلين إمّا من عائلتك أو أصدقائك أو غيرهم، وكذلك لحمايته مبدئيًا - ولو بصورة طفيفة فقط - من اللصوص الذين قد يسرقون حاسوبك المحمول ويحاولون فتحه. يمكنك إعداد كلمة المرور أو تغييرها من الإعدادات (Settings) --> الحسابات (Accounts) --> خيارات تسجيل الدخول (Login Options) --> كلمة المرور (Password).

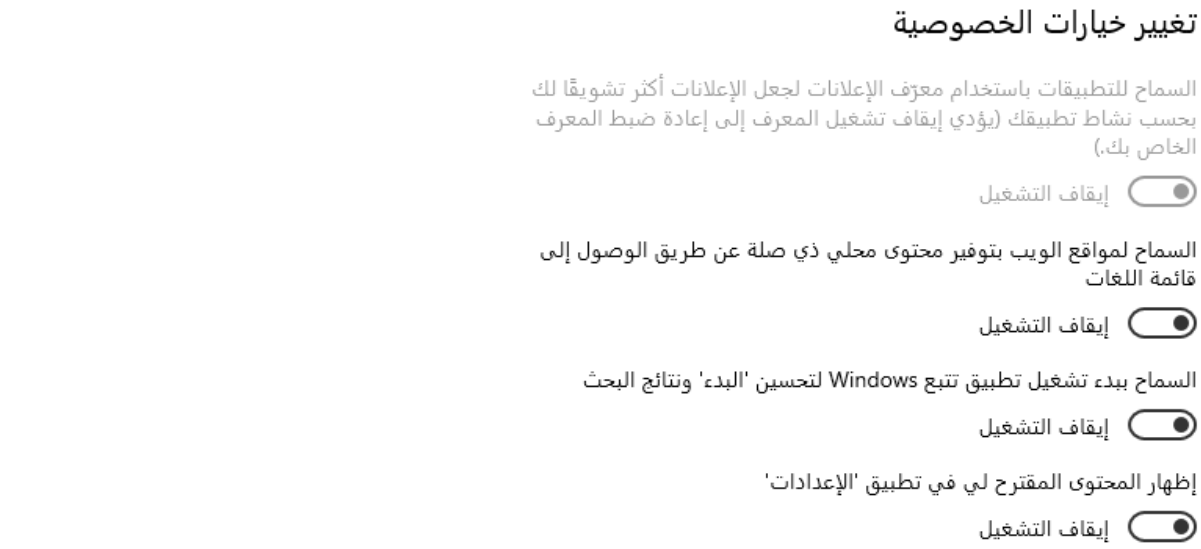
قم كذلك بتفعيل الخيار التالي كما في الصورة لتفعيل قفل الشاشة وطلب كلمة المرور تلقائيًا عندما تكون بعيدًا عن حاسوبك لفترة من الزمن:



6. 1. 3. تعطيل إعدادات مشاركة البيانات

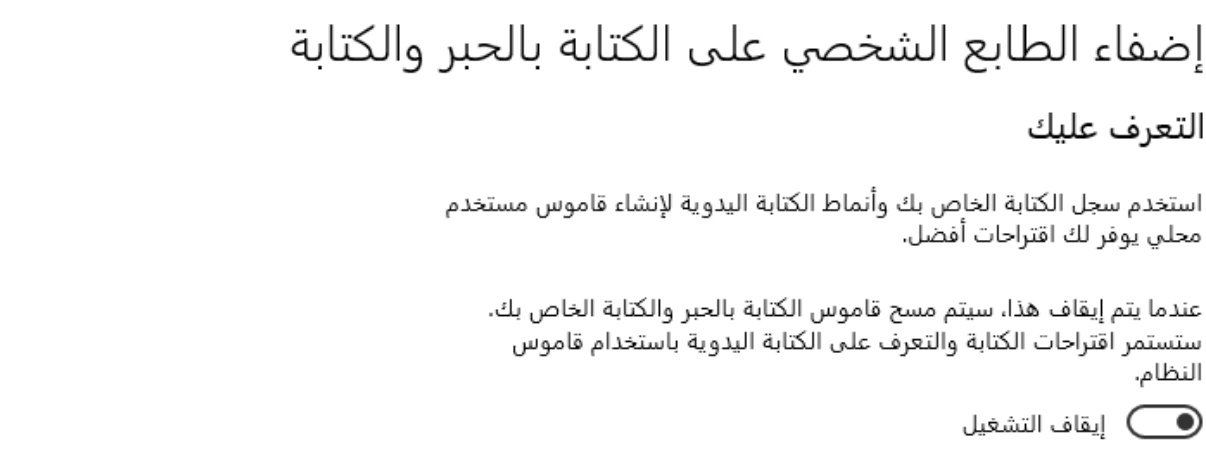
ويندوز 10 افتراضيًا ممتلئ جدًا بإعدادات إرسال البيانات إلى مايكروسوفت. عليك تعطيلها جميعًا لتقليل البيانات المُرسلة من جهازك إلى خواديم الشركة.

من الإعدادات (Settings) --> الخصوصية (Privacy) --> عام (General)، تأكّد أنّ إعداداتك هي كالشكل التالي:



عطّل خدمة التمييز الصوتي من تبويب الكلام (Speech):

عطّل خدمة الاحتفاظ بالكلمات التي تكتبها من تبويب إضفاء الطابع الشخصي على الكتابة بالحبر والكتابة (Inking & Typing Personalization):



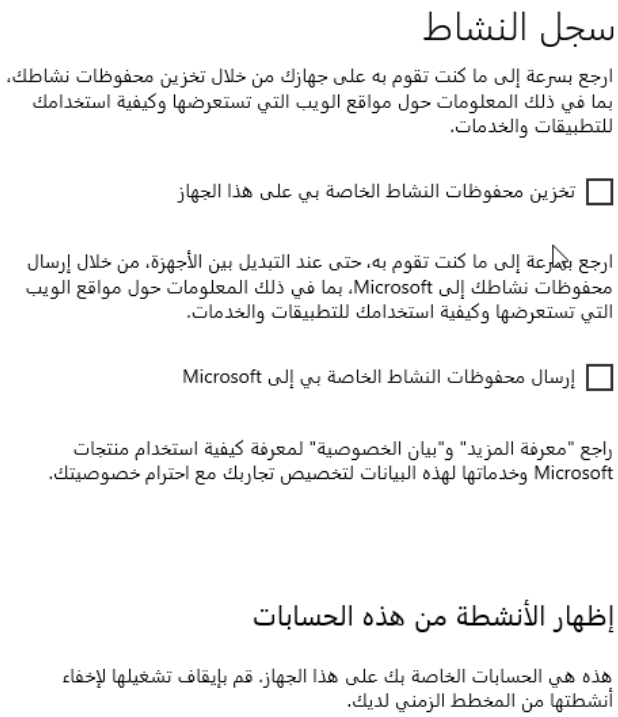
تأكّد أنّ وضع إرسال البيانات عن حاسوبك مضبوطٌ إلى أساسي (Basic) من تبويب التعليقات والتشخيص (Diagnostics & Feedback). سيظل حاسوبك هكذا يرسل البيانات عنك للأسف ولا يمكن تعطيل إرسال البيانات بصورة كاملة في ويندوز 10، لكن البيانات المُرسلة أقل من الوضع الآخر:

تأكّد أنّ بقية الخيارات في الصفحة كالتالي:

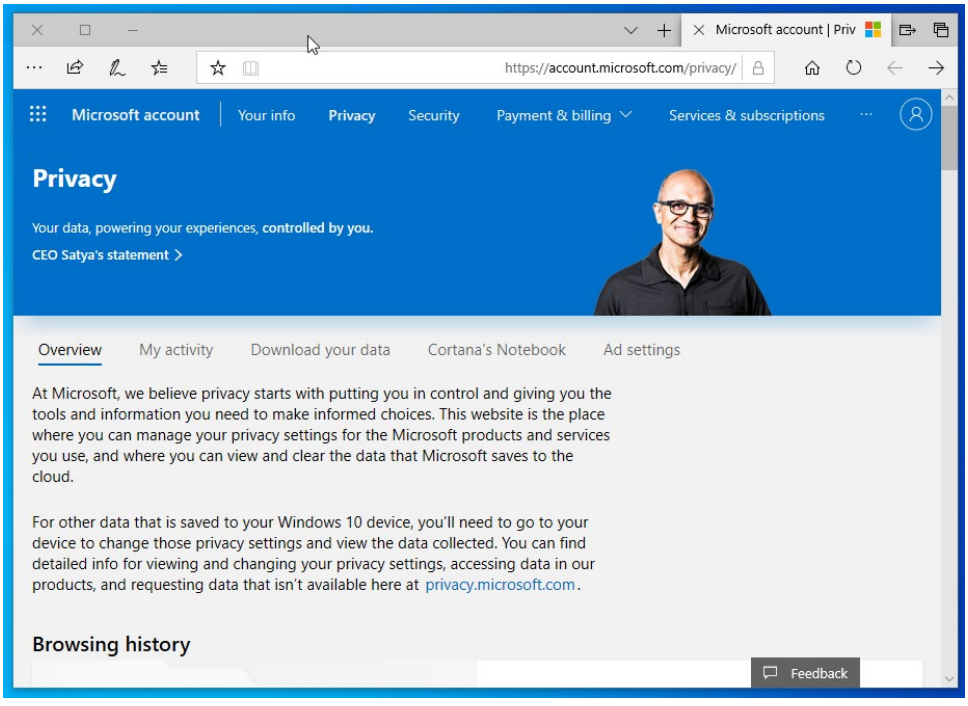
يسـمح لـك الخيـار الأخيـر أن تثبّـت برنامجًـا اسـمه "Diagonstic Data Viewer" أو "عـارض بيانـات التشـخيص" وهـو برنامـجٌ رسـمي مـن مايكروسـوفت لعـرض كلّ البيانـات الموسّـعة (لا يعـرض كلّ البيانـات بـل فقـط عنـد اسـتخدام نمـط الإرسـال الموسّـع) التـي تُرسـل مـن جهـازك إلـى مايكروسـوفت. ينبغـي أن يكـون فارغًـا عندمـا تفتحـه:

يمكنـك حـذف كل البيانـات التشـخيص التـي جمعتهـا عنـك مايكروسـوفت إن أردت، كمـا يمكنـك كذلـك تعطيـل خيـار طلـب سـؤالك عـن تقييمـك للنظـام كلّ فتـرة مـن نفـس الصفحـة:

تأكّد أنّ خيارات الاحتفاظ بنشاطك على جهازك معطّلة من تبويب سجل النشاط (Activity History):

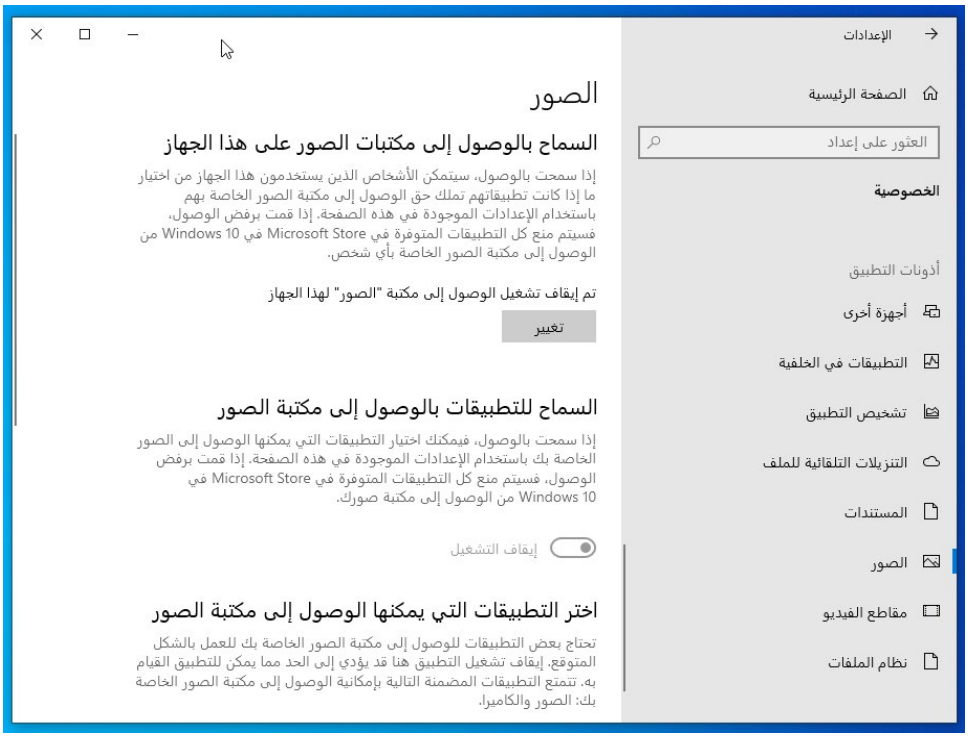


إذا كنت تستخدم حسابًا من مايكروسوفت لتسجيل الدخول إلى نظام التشغيل الخاصّ بك فيمكنك رؤية كلّ المعلومات التي جمعتها عنك مايكروسوفت من الرابط: https://account.microsoft.com/privacy وبعد أن تقوم بتسجيل الدخول إلى حسابك هناك سترى بياناتك ومعلوماتك مقسّمةً حسب نوعها. يمكنك رؤيتها أو حذف ما تشاء منها أو حتّى تنزيلها إن أردت:



بقية التبويبات التي تراها هي صلاحيات الوصول للتطبيقات الموجودة على نظامك، يمكنك تصفّح كلٍّ منها على حدى:

جميع هذه التبويبات تحوي خياراتٍ لتفعيل الصلاحية المذكورة في اسمها بالإضافة إلى إمكانية السماح أو منع تطبيقاتٍ معيّنة فقط من تلك الصلاحيات. ما ننصح به هو أن تمرّ عليها جميعًا وتقوم بتعطيل جميع الصلاحيات عبر تغييرها من On إلى Off، إلّا تلك التي تحتاج إليها تطبيقاتك الأساسية (مثلًا بالنسبة لصلاحيات الميكروفون، يمكنك ترك السماح للتطبيقات بالوصول إليه، لكن مع منع جميع التطبيقات من استخدامه إلّا متصفّح الويب الخاصّ بك والألعاب مثلًا):

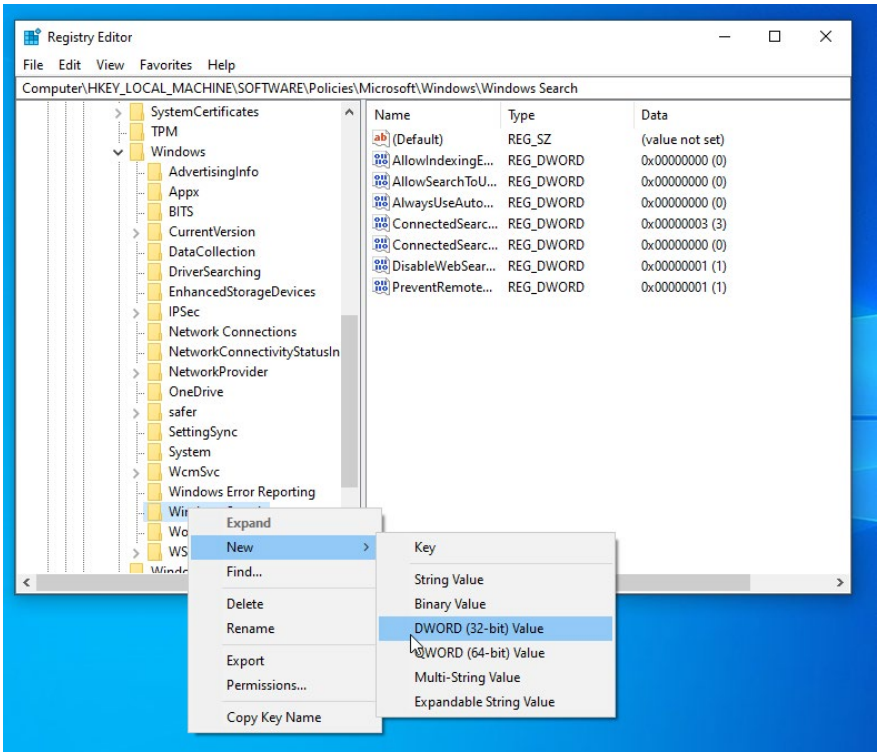


6. 1. 4. تعطيل المساعدة الصوتية (Cortana)

كورتانا هي مُساعِدة صوتية موجودة داخل ويندوز 10، تسمح لك بالبحث عن بعض الأشياء على جهازك أو الويب صوتيًا، أو يمكنك حتّى أن تسألها بعض الأسئلة خارج ذلك، مثل لماذا أهالي الفتيات يطلبون مهورًا عالية للزواج؟ :)

اتّبع الخطوات التالية لتعطيل كورتانا:

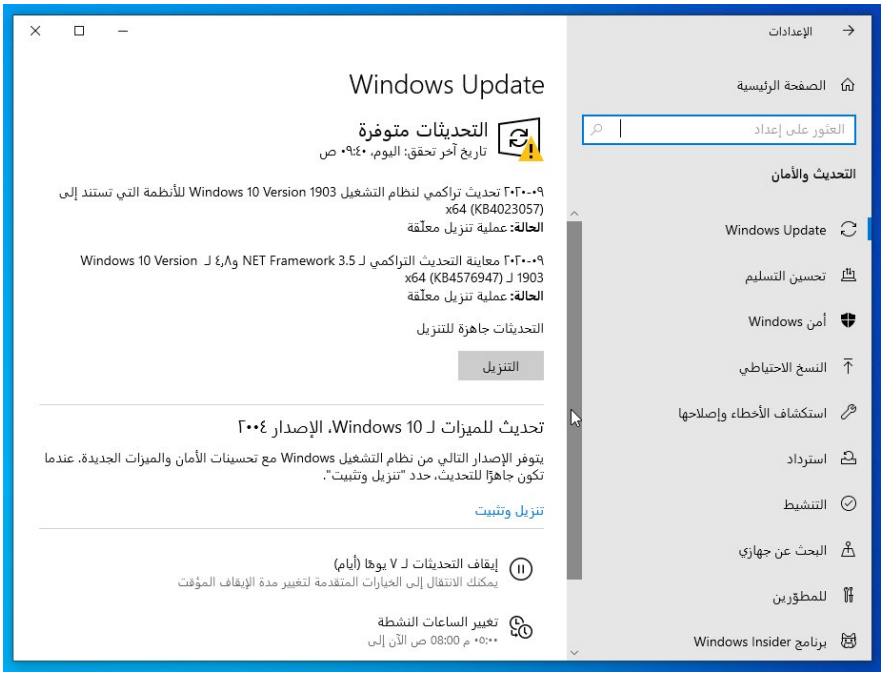
1. انقر بزرّ الفأرة الأيمن على أيقونة ويندوز واختر "Run" واكتب "regedit".
2. اذهب إلى المسار التالي من الشريط الجانبي: HKEYLOCALMACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search
3. انقر على Windows Search بزرّ الفأرة الأيمن، واختر New --> New DWORD (32 Bit) كما في الصورة:



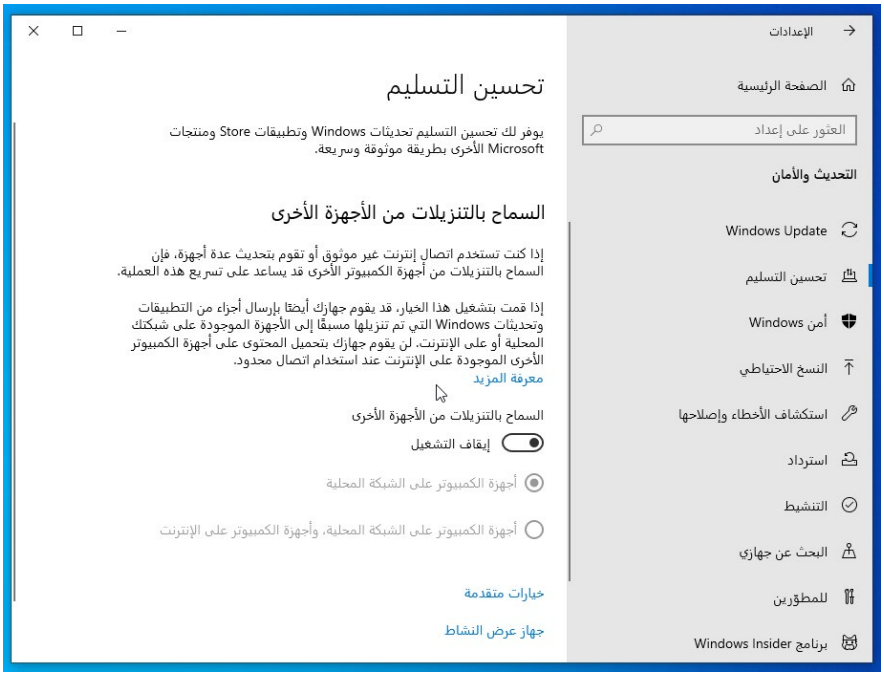
4. أدخل "AllowCortana" كاسم القيمة الجديدة.
5. أعد التشغيل.

6. 1. 5. إدارة التحديثات

التحديثات مفعّلة تلقائيًا على ويندوز 10، لكن أحيانًا تكون عالقة عند خطوة معيّنة وتتطلب منك تنزيلها يدويًا. يمكنك التحقق من حالة التحديثات الحالية على نظامك عبر الإعدادات (Settings) --> التحديث والأمان (Update & Security) وتثبيت أيّ تحديثاتٍ عالقة:



ننصح كذلك بتعطيل ميّزة تحميل التحديثات من الأجهزة الأخرى عبر الشبكة من تبويب تحسين التسليم (Delivery Optimization) بالشكل التالي، وهذا لعدم حصول مشاكل في الشبكة المنزلية من تنزيلٍ ورفعٍ للتحديثات:



6. 1. 6. تفعيل Windows Defender والجدار الناري

اذهب إلى الإعدادات (Settings) --> التحديث والأمان (Update & Security) --> أمن Windows (Windows Security) وشغّل مركز حماية ويندوز من هناك:

اذهب إلى تبويب أنشطة جدار الحماية والشبكة (Firewall & Network Protection) ومن الشريط الأيمن انقر على إدارة الموفرون (Manage Providers)، ثمّ تأكّد أنّ كلًّا من الجدار الناري و Windows Defender مفعّلان بالشكل التالي:

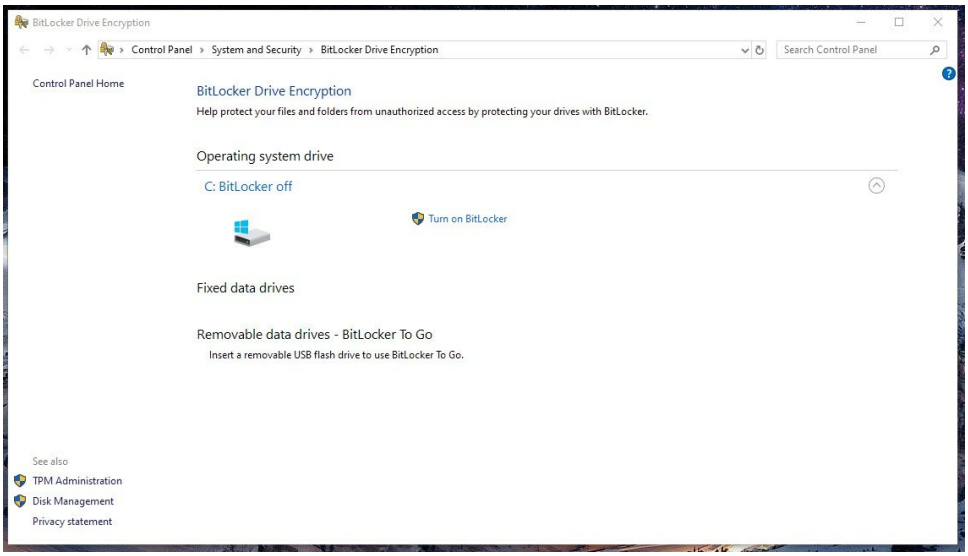
لا يحتاج ويندوز 10 أيّ برنامج مكافحة فيروسات على عكس ما يعتقده الناس في الواقع.

طالما أنّك ملتزمٌ بتعليمات الوعي والأمان التي شرحناها في فصولٍ سابقة فحينها لست بحاجة لبرنامج مكافحة فيروسات سوى الموجود داخل ويندوز نفسه. عليك فقط تجنّب تحميل البرمجيات من مصادر مشبوهة وتجنّب إدخال ذواكر USB خبيثة إلى جهازك.

6. 1. 7. تشفير الأقراص أو المجلدات

تسمح لك ميّزة "Bitlocker" الموجودة داخل ويندوز 10 بتشفير كامل القرص الصلب الخاصّ بك. وهذه ميّزة رائعة فالتشفير يضمن لك أنّ أحدًا لن يصل إلى ملفّاتك في الكثير من الحالات، وحتّى لو سُرق الحاسوب منك فسيظل السارق غير قادرٍ على الوصول إلى البيانات الموجودة فيه لأنّ القرص الصلب مشفّر (باستثناء ما إذا كان الحاسوب المحمول يعمل مثلًا أثناء سرقته، فحينها قد يتمكّن المخترقون من سحب البيانات عبر الذاكرة العشوائية عبر أساليب متقدمة جدًا، لكنّ هذا بعيدٌ عن تفكير أبوعبّود الحرامي الموجود في حارتكم غالبًا).

لتفعيل Bitlocker، اذهب إلى لوحة تحكّم ويندوز وببساطة اكتب "Bitlocker" في مربّع البحث وافتحه:



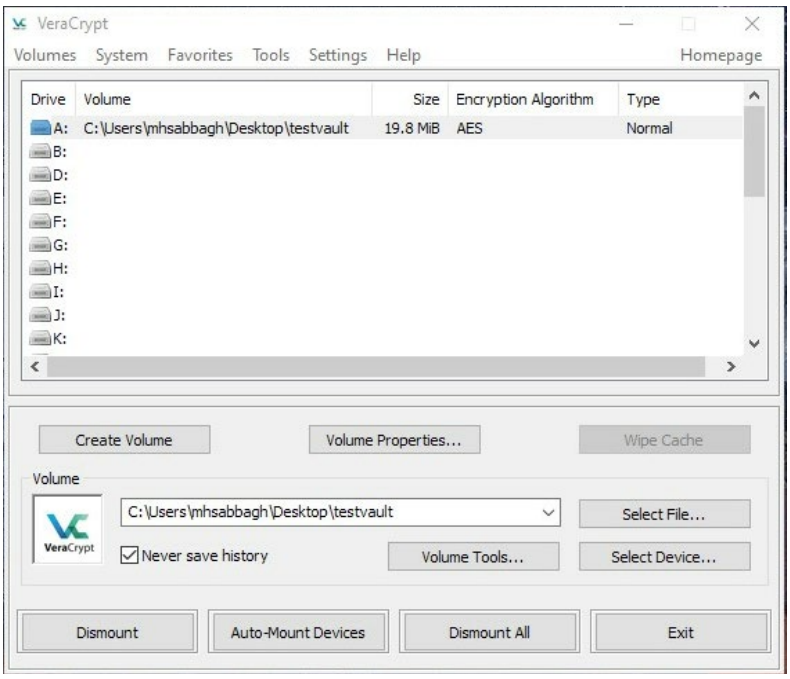
انقر على زرّ تفعيل Bitlocker أو "Turn on Bitlocker" الذي تراه بالصورة للقرص الذي تريد تشفيره، ثمّ تابع العملية.

- إذا سألك عن نوع التشفير الذي تريده، اختر "Encrypt Entire Drive" أو "تشفير كامل القرص". وهذا لضمان تشفير جميع ملفّاتك وليس الجديد منها فقط.
- إذا سألك عن مكان حفظ مفتاح الاسترجاع (Restore Key)، فيمكنك إمّا طباعته أو نسخه إلى ملفّ تخزّنه في مكانٍ آمن.

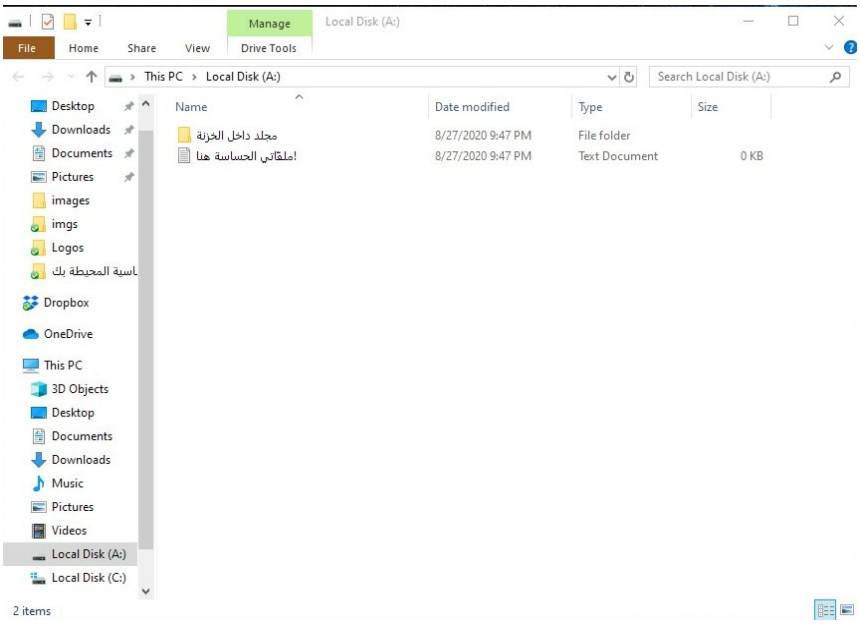
قد تستغرق العملية بعض الوقت، بعدها ستحتاج إعادة التشغيل ليكتمل التشفير، وسيطلب منك النظام إدخال كلمة المرور التي أدخلتَها أثناء قيامك بإعداد Bitlocker.

لا يعمل Bitlocker على الأنظمة المُقرصنة (Cracked) من ويندوز، كما قد يحتاج تفعيل بعض الخيارات من نظام الـBIOS الخاصّ بالجهاز تُدعى TPM قبل القيام بالعملية. كما لا يعمل جيّدًا على الحواسيب التي تحوي نظاميّ ويندوز ولينكس معًا (يحتاج فقط أن يكون ويندوز مسيطرًا على محمّل الإقلاع الرئيسي للجهاز).

كلّ ما سبق هو لتشفير كامل القرص الصلب، لكن ربّما تريد تشفير بعض الملفّات والمجلّدات فقط عوضًا عن ذلك، والحلّ حينها عبر استخدام برامج خارجية مثل VeraCrypt وغيرها. تسمح لك هذه البرامج بإنشاء أقراص صغيرة محلّية (هي في الواقع عبارة عن ملفّات حاويات) داخل نظامك الحالي لتقوم بوضع ملفّاتك الحساسة داخلها. فكّر بها على أنّها مثل "الخزنة" (Vault) داخل نظامك، وهي محمية بكلمة مرور وتستعمل تشفيرًا قويًا، وهكذا لا يمكن لأحدٍ فتحها إلّا إن امتلك كلمة المرور. يمكنك إنشاء هذه الأقراص لتكون بأيّ حجمٍ تريده وتحتاج إليه:



كلّ ما عليك فعله بعد أن تنشئها هو أن تضع ملفّاتك المهمّة داخلها، تمامًا كما تفعل داخل أيّ مجلّد:



هذه الملفّات والمجلّدات محمية بكلمة مرور، وبالتالي لا يمكن لأحد فتحها سواك. يمكنك أخذ هذه الخزنة ووضعها في مجلّد عميق داخل نظامك بحيث لا يعرف أحدٌ أنّها موجودة حتّى للمزيد من من الحماية.

6. 1. 8. حذف الملفات نهائيًا

عندما تحذف الملفّات من نظام التشغيل فأنت لا تحذفها بصورة نهائية مباشرةً، بل ما يقوم نظام التشغيل بفعله هو أنّه يزيل الارتباط ما بين نظام الملفّات (Filesystem) وبيانات الملفّ فقط، ولا تُحذف بيانات الملفّ بالكامل إلّا بعد أن تأتي بياناتٌ جديدة لتكتب فوق نفس المساحة التي كانت مخصصة من قبل للملفّ القديم.

وهذا هو المبدأ الذي تقوم عليه برامج الاستعادة (Restore Programs) التي تحاول استعادة الملفّات المحذوفة. وهذه مشكلة للكثير من الناس الذين يبيعون حواسيبهم وهواتفهم المحمولة ولا يدركون أنّ ملفّاتهم ربّما ما تزال قابلة للاستعادة من طرف المشترين الجدد بعد أن يبيعوها.

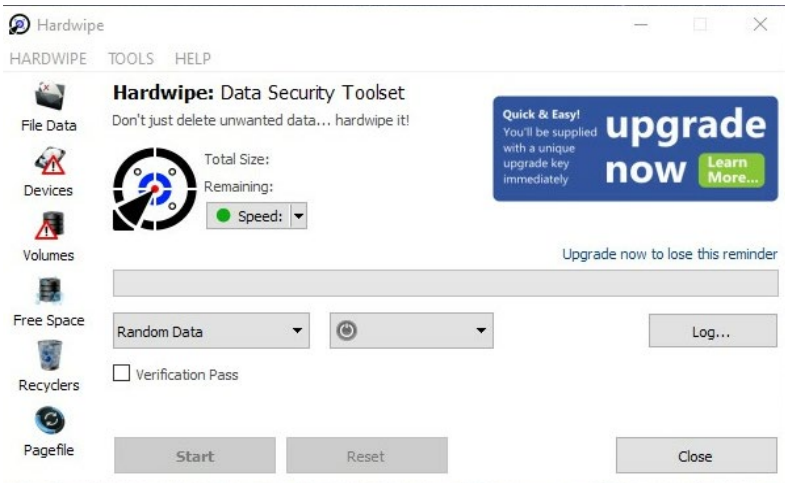
وهذا الأمر وإن كان جميلًا لاستعادة بعض ملفّاتك التي حذفتَها عن طريق الخطأ إلّا أنّه سيء للأمان الرقمي خصوصًا إن كنتَ في بيئةٍ خطرة وتريد حذف الملفّات نهائيًا بلا رجعة. وهناك برمجيات متخصصة في حذف الملفّات والأقراص لحلّ هذه المشكلة؛ حيث تحدد الملفّات والمجلّدات والأقراص الصلبة التي تريد حذفها بصورة نهائية بلا رجعة وتتكفّل هذه البرامج بالقيام بالعملية.

لكن هناك مشكلة كبيرة فيما يتعلق بحذف الملفّات بصورة نهائية، وهي أنّه تقريبًا من المستحيل ضمان حذفها على الأقراص الصلبة الثابتة (Solid-State Drives - SSD) وبطاقات SD Cards، وهذا لأنّ هذا النوع من أقراص التخزين يضرّه كثرة الكتابة فوق نفس المكان على القرص،

فيحتوي تقنيةً تقوم تلقائيًا بتوزيع البيانات الجديدة إلى أماكن متفرّقة على القرص لإطالة عمره الافتراضي [1]. وهذا يجعل كلّ برامج حذف البيانات غير فعّالة حقيقةً عليه، لكنّها قد تساعد بصورة طفيفة. وتشفير كامل القرص الصلب هو الحلّ الحقيقي لحذف الملفّات كما شرحنا في خطوةٍ سابقة، وبعدها يمكنك حذف الملفّات بصورة عادية دون قلق.

نكرر: لا تعمل برمجيات الحذف على أقراص الـSSD وبطاقات SD Cards بصورة جيدة لضمان حذف الملفّات بصورة دائمة. لكنّ استخدامها أفضل من لا شيء، إن كان اللاشيء هو البديل لديك.

من بين البرامج المُساعِدة HardWipe وEraser، وهي برمجيات سهلة الاستخدام؛ فكلّ ما عليك فعله هو اختيار المجلّدات والملفّات المطلوبة:



لاحظ أنّه لا يمكنك حذف الأقراص الخاصّة بالنظام التي قيد الاستخدام حاليًا بصورة كاملة عن طريق هذه البرامج؛ فإذا كنتَ تريد مثلًا بيع حاسوبك وبالتالي تريد حذف كلّ شيءٍ موجودٍ على القرص الصلب فحينها عليك استخدام طُرقٍ أكثر تقدّمًا، مثل أن تثبّت أحد توزيعات لينكس على ذاكرة USB ثمّ تقلع منها ثمّ تحذف كامل القرص الصلب عن طريقها (سنشرحها في قسم تأمين أنظمة لينكس).

6. 2. تأمين أنظمة لينكس

أنظمة لينكس لسطح المكتب - وبالتحديد توزيعات مثل أوبونتو ولينكس منت - آمنة وتحترم الخصوصية افتراضيًا على عكس أنظمة ويندوز ومماك. لا يوجد إرسال بيانات ولا تعقّب ولا أي شيء لتعطّله افتراضيًا (هناك إمكانية لتعطيل خيار بسيط لإرسال معلومات العتاد عن جهازك إلى كانونيكال، لكنك غالبًا رأيته بنفسك بالفعل فهو يُعرَض عليك أثناء التثبيت).

ما يزال هناك بعض النقاط لتأخذها في الحسبان.

6. 2. 1. استخدام مستودعات آمنة

تدعم توزيعات لينكس ما يُعرف بالمستودعات (Repositories)، والمستودعات هي مصادر البرمجيات التي يمكنك منها تحميل ما يعرف بالحِزَم (Packages). تمتلك توزيعات لينكس الرئيسية مثل أوبونتو ولينكس منت أكثر من 50 ألف حزمة داخل مستودعاتها الرسمية.

قد تكون بعض البرمجيات أحيانًا غير موجودة في المستودعات الرسمية، وعند بحثك عنها على الشبكة تجد أنّ مطوريها يقترحون عليك إضافة مستودعاتهم الخاصّة إلى نظامك من أجل تثبيت برمجياتهم. هذا به مشكلة لأنّ:

- بمجرّد إضافة مستودعٍ ما إلى نظامك فقد سمحتَ لأصحاب المستودع أن يصلوا إلى كامل نظامك، فيمكنهم مثلًا - من ناحية القدرة - جعل التحديث القادم يحذف كلّ ملفّاتك، أو يشفّرها أو يرسلها إليهم.
- لا تضمن أنّ هذه البرمجيات الخارجية لا تحوي برمجيات خبيثة أو برمجيات تجسس أو ثغرات أمنية بسبب الاعتماديّات (Dependencies) الموجودة فيها.
- لا تضمن كذلك أنّ هذه البرمجيات لا تتعارض مع إصدارات الاعتماديّات الموجودة في نظامك، فتخرّبه دون أن تدري.

ننصح بسبب ذلك ألّا تقوم بإضافة مستودعاتٍ خارجية إلى نظامك إلّا على أضيق نطاق، ومن أشخاصٍ أو مؤسسات تعرفهم بصورة قوية قبل أن تقوم بذلك. لا تكتفي برؤية المستودع على أحد مدونات الإنترنت فتقوم بإضافته إلى نظامك.

إن لم تعرف هل هذا المستودع آمن أم لا، فيمكنك سؤال الخبراء على منصّات المساعدة الشهيرة على الإنترنت وانتظار جوابهم.

6. 2. 2. إدارة التحديثات

تتبع توزيعات لينكس منهجًا مختلفًا فيما يتعلّق بالتحديثات.

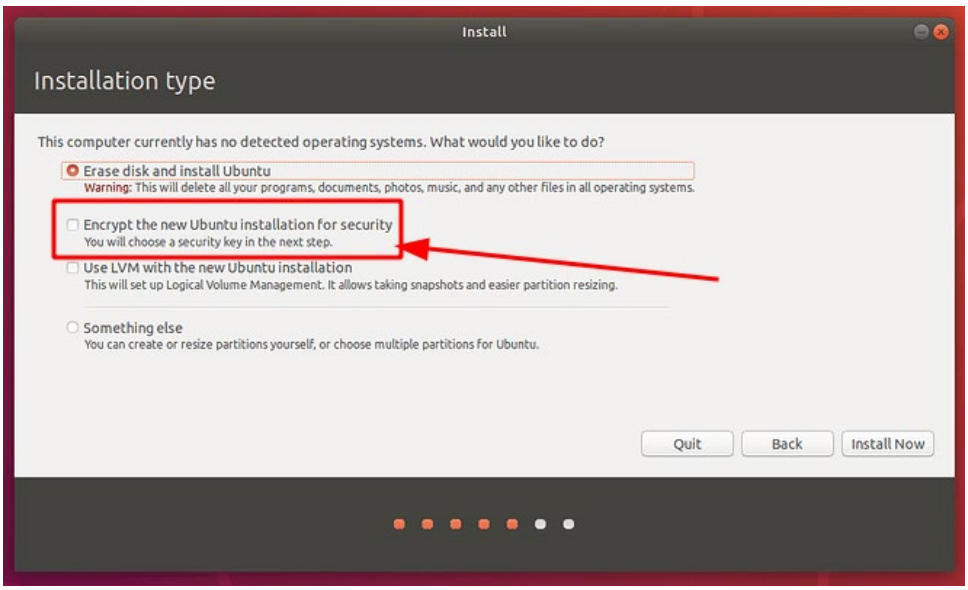
تُثبّت التحديثات الأمنية المهمّة فقط تلقائيًا على أوبونتو ولينكس منت، وعدا عن ذلك يبقى الأمر متروكًا للمستخدم ليثبّت التحديثات متى ما شاء. يمكنك البحث عن التحديثات الحالية أو تثبيتها من برنامج مدير التحديثات (Update Manager):

هناك ما يعرف بـ"Snaps" على الإصدارات الأخيرة من أوبونتو، وهي حزم من نوع خاصّ لا تتبع تحزيم البرمجيات dpkg ولا تأتي بصيغة .deb، بل تُثبّت من متجر السناب (Snap Store) الخاصّ بشركة كانونيكال (Canonical) المطوّرة لأوبونتو. وهي برمجيات مُحتواة داخل حاويات (Containers) تحوي اعتمادياتها كلّها في حزمة واحد. جميع تحديثات السناب تلقائية تجري بالخلفية وقت حصولها، بل لا يمكنك تعطيلها حتّى.

ننصح بتثبيت آخر التحديثات المتوفّرة بصورة أسبوعية على الأقل بشدّة.

6. 2. 3. التشفير

عند تثبيتك لتوزيعة لينكس مثل أوبونتو ولينكس منت، هناك خيارٌ يسمح لك بتشفير كامل القرص الصلب، ننصح باستخدامه بشدّة فهو أسهل شيء لضمان حماية بياناتك:



سيتوجّب عليك اتباع خطواتٍ أكثر من ذلك إذا انتهيت من التثبيت بالفعل ونسيت تفعيل التشفير لتفعيله وهي فوق المستوى العادي لقرّاء هذا الكتاب. ننصح بأخذ نسخة احتياطية من ملفّاتك المهمّة ثم حذف نظامك وتثبيته من جديد مع تفعيل خيار التشفير المذكور أثناء التثبيت، فهو أسهل من محاولة تفعيل التشفير بعد التثبيت.

إن تشفير الملفّات يحميك من معضلة حذف الملفّات بصورة نهائية على أقراص الـSSD - كما ستقرأ في القسم التالي - وهذا لأنّ التشفير يُطبّق كذلك على الملفّات المحذوفة، وبالتالي تصبح استعادتها شبه مستحيلة من طرف جهة ثالثة.

إن لم تُرد تشفير كامل قرصك الصلب فيمكنك على الأقل استخدام برنامج VeraCrypt إن أردت لإنشاء "خزنات" (Valuts) آمنة، حيث تضع فيها الملفّات التي تريد تشفيرها وحمايتها بكلمة مرور. البرنامج يعمل على جميع توزيعات لينكس ويمكن تحميله من موقعه الرسمي.

6. 2. 4. حذف الملفات والأقراص بصورة نهائية

لا تُحذَف الملفّات والأقراص بصورة نهائية على لينكس تمامًا كما على ويندوز، وتحتاج استخدام برمجيات إضافية للقيام بالعملية. وهنا تبرز نفس المشكلة حيث لا يمكن حذف الملفّات بصورة نهائية على أقراص SSD.

لكن ما يمكنك فعله - إن أردت - هو حذف الأقراص كاملةً والكتابة فوقها ببيانات عشوائية. هذا يزيد من فرصة تدمير البيانات للأبد بصورة كبيرة، لكن بالطبع ستخسر كلّ بياناتك (يمكنك تطبيقها عبر الإقلاع من ذاكرة USB مثلًا، وهي مفيدة في حال أردت بيع حاسوبك):

```
sudo dd if=/dev/urandom of=/dev/sdX bs=4096 status=progress
```

مع استبدال sdX بالقرص المُراد حذفه بالكامل (استعمل sudo fdisk -l لسرد الأقراص المتوفّرة ثمّ انظر أيّ الأقراص تريد حذفه). إليك ما يفعله هذا الأمر:

- dd هو اسم البرنامج، يجب استعماله مع صلاحيات الجذر (sudo) للكتابة على الأقراص.
- if=/dev/urandom نقوم هنا بتحديد مصدر البيانات المُدخلة، وif هي اختصار لـInput file. توجد على لينكس بعض المسارات التي تولّد بيانات عشوائية بصورة مستمرة لبعض الاحتياجات الخاصّة مثل /dev/zero و /dev/urandom، يقوم هذا الأخير بتوليد أرقام عشوائية بصورة غير محدودة. ونستفيد منها نحن هنا بأخذها والكتابة فوق قرص الـSSD بالكامل وفقًا لحجمه تلقائيًا. (مثلًا إذا كان حجمه 300 جيجابت، فما سيحصل هو أنّ الأمر

سيكتب 300 جيجابت من البيانات العشوائية على القرص لضمان إزالة البيانات السابقة).

- of=/dev/sdX نحدد هنا القرص المُراد الكتابة عليه، وof هي اختصار لـOutput File.
- bs=4096 تعليمة مُساعدة بسيطة، تُخبر البرنامج أن يكتب 4096 بايت من البيانات في الوقت نفسه.
- status=progress نطلب هنا من البرنامج أن يعرض شريط التقدّم لنا لنعرف أين وصل أثناء تطبيق الأمر.

يمكنك كذلك مراجعة صفحة Solid State drive/Memory Cell clearing على موسوعة أرتش لينكس للمزيد من إرشادات حذف بيانات SSD بالكامل على مختلف أنواع تلك الأقراص في السوق.

إذا كنتَ تريد حذف الملفّات بصورة عادية فحينها عليك استخدام التشفير كما في الخطوة السابقة، ثمّ حذف الملفّات والمجلّدات كما تفعل عادةً. عدا عن ذلك لن يكون هناك ضمان.

6. 2. 5. إزالة تاريخ الأوامر

هناك ملفّ اسمه .bash_history وهو موجودٌ في مجلّد المنزل الخاصّ بك على كل توزيعة لينكس. يحوي هذا المجلّد كلّ الأوامر التي طبّقتها من قبل على نظامك منذ تثبيته. وهذا قد يشكّل خطرًا أمنيًا بناءً على نوعية الأوامر التي تكتبها وهل تتضمن معلومات حسّاسة أم لا (ولهذا يُستحسن بالمناسبة عدم كتابة كلمات المرور بصورة صرفة داخل الأوامر مهما كان السبب).

وهذه هي الميزة التي تسمح للمستخدم أن يفتح الطرفيّة (Terminal) ويضغط على زرّ السهم العلوي على لوحة المفاتيح، فيظهر له آخر أمر قام بتطبيقه على نظامه، وهكذا إلى أن يصل إلى بقيّة الأوامر.

كلّ ما عليك فعله هو حذف الملفّ كل بضعة أسابيع أو شهور حسبما تحتاج:

```
rm ~/.bash_history
```

6. 3. تأمين جهاز الـRouter (الموجه) والشبكات اللاسلكية

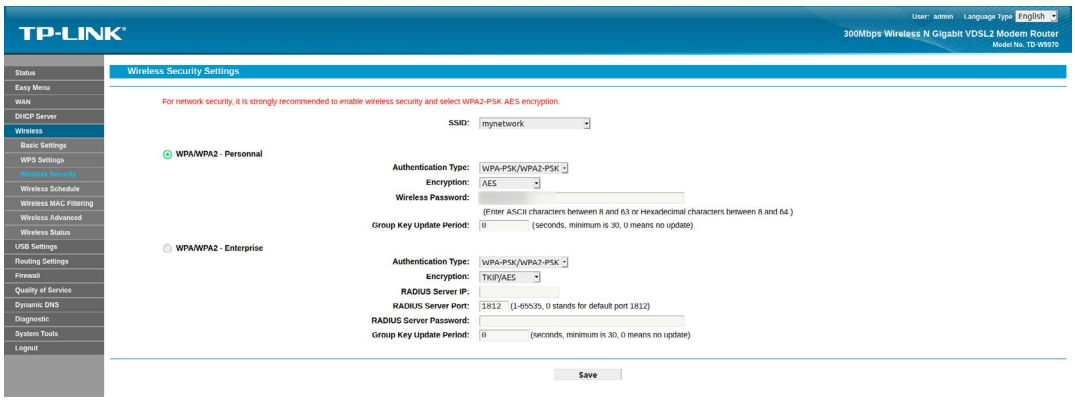
غالبًا ما يعطيك موظّف مزوّد خدمة الإنترنت (Internet Service Provider - ISP) اسم المستخدم وكلمة المرور الخاصّين بالموّجه أو الراوتر (Router) عندما يقوم بتركيب الإنترنت في منزلك لأوّل مرّة. يمكنك الوصول إلى لوحة تحكّم الموجّه عبر العنوان 192.168.1.1 داخل

متصفّحك (غالبًا هذا هو على معظم أجهزة الموّجهات، لكن يمكن أن يختلف أحيانًا ويمكنك أن تتأكّد منه من دليل استخدام الموجّه أو من العلبة التي يأتي بها). إن لم يزوّدك بهذه البيانات فيمكنك البحث عنها على الإنترنت عبر كتابة اسم طراز الموجّه ورقمه في محرّك البحث، وغالبًا ما يكون admin/admin في المرّة الأولى.

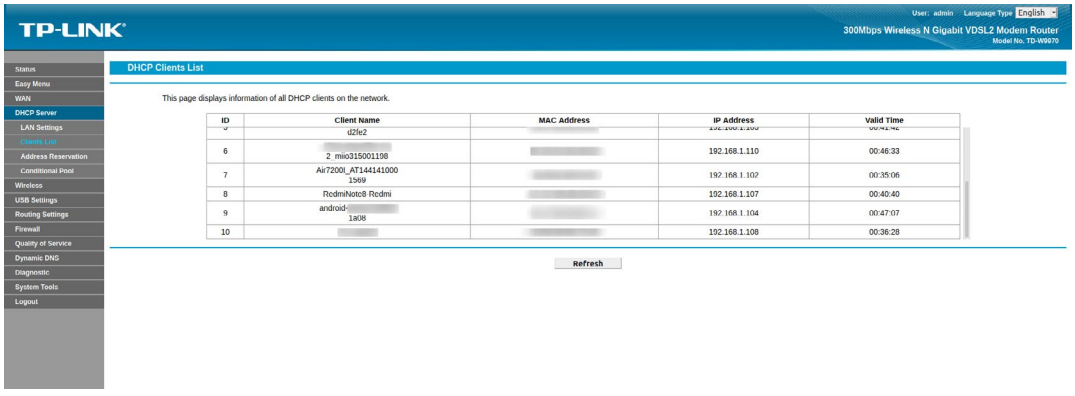
عليك القيام بعدّة أشياء لتأمين شبكتك المنزلية بعد أن تفتح لوحة تحكّم الموجّه. تختلف أماكن هذه الأشياء بناءً على الشركة المصنّعة للموجّه ونوعه وطرازه.

أوّلًا، قم بتغيير اسم المستخدم وكلمة المرور الخاصّين بتسجيل الدخول إلى لوحة التحكّم، وهذا لمنع المخترقين من الوصول إلى كامل إعدادات شبكتك المنزلية في حال نجحوا - فرضًا - باختراق شبكة الاتصال اللاسلكية في منزلك. يمكنك القيام بذلك من تبويب إدارة المستخدمين الخاصّ بالموجّه لديك.

ثانيًا، قم بتغيير اسم شبكة الاتصال اللاسلكي وكلمة المرورّ الخاصّة بها. وهذه عملية سهلة جدًا من لوحة التحكّم. قم كذلك باستخدام تشفير WPA-2 في طلب منك الموجّه تحديد نوع التشفير. اتبع إرشادات كلمات المرور القوية التي سنذكرها في فصل "كلمات المرور" لاحقًا:

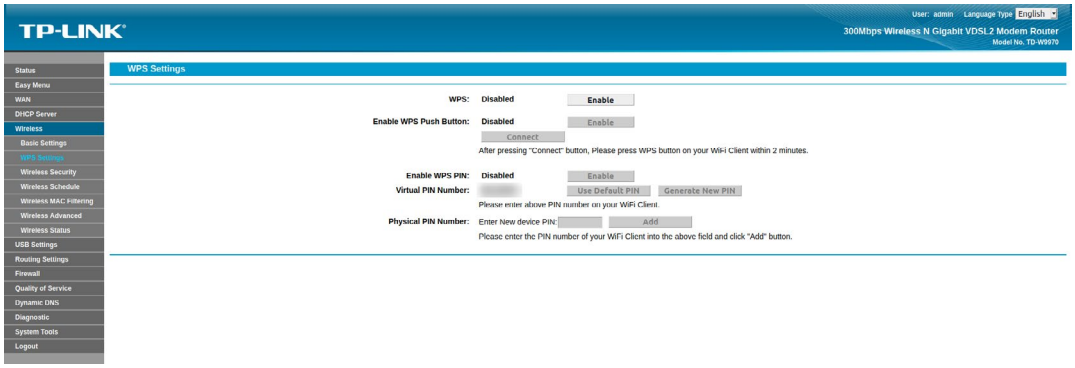


ثالثًا، هناك غالبًا صفحة تسمّى DHCP Clients أو اسمًا شبيهًا بذلك تريك كلّ الأجهزة المتصلة بالشبكة اللاسلكية الحالية مثل هذا الشكل:



يمكنك التأكّد عبرها من أنّ أجهزتك فقط هي المتصلة بالشبكة اللاسلكية، فإذا كان لديك 4 أجهزة فقط في المنزل بينما هناك 7 أجهزة متصلة مثلًا، فحينها هذا يعني أنّ أحدهم قد اخترق شبكة الاتصال اللاسلكية الخاصّة بك ويستخدمها مجانًا على حسابك.

أخيرًا، عليك إيقاف ما يعرف بميّزة WPS، وهي ميّزة موجودة داخل معظم الموجّهات. تسمح هذه الميّزة لمختلف الأجهزة بالاتصال بالشبكة اللاسلكية إمّا عبر ضغط زرٍ موجود على الموجّه نفسه عندما تريد ربط جهازك بالشبكة، أو عبر رقمٍ سرّي مكوّنٍ من 8 أرقام تدخله في جهازك عندما تريد ربطها بالشبكة. الطريقة الأولى أكثر أمانًا ولكنّها تسمح لأي شخص أن يشترك بالشبكة بمجرّد ضغط الزرّ، أمّا الثانية فهي كارثية لأنّها تفتح المجال لهجمات القوّة الوحشية (Bruteforce) حيث أنّ كسر الكلمة المكوّنة من 8 أرقام سهلٌ جدًا. يمكنك تعطيل WPS من خيارات الشبكة اللاسلكية:

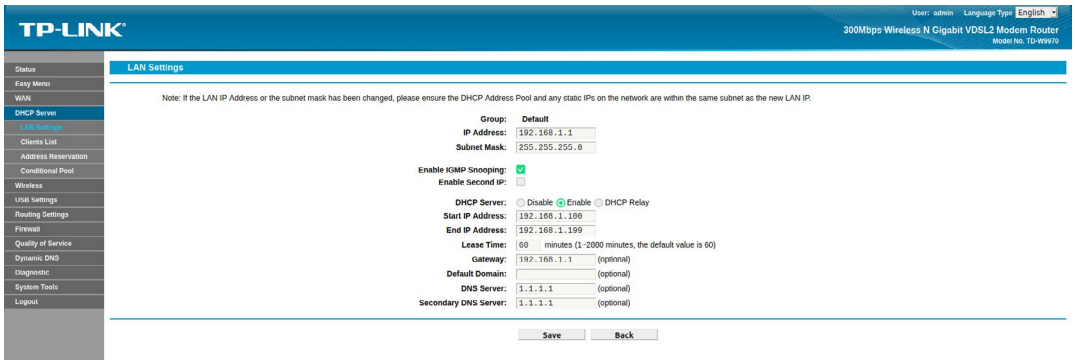


عليك تغيير كلمة مرور الشبكة اللاسلكية كلّ فترة؛ لا تتركها لمدّة سنوات دون تغيير. بل يستحسن أن تقوم بتغييرها كلّ بضعة أشهر بنفسك.

6. 3. 1. استخدام DNS للحماية

يمكنك استخدام أحد مزوّدات خدمة أسماء النطاقات (DNS) التي تقوم بتسريع التصفّح وحجب المواقع الإباحية والخبيثة داخل الموجّه الخاصّ بك، وهكذا تضمن أنّ جميع أجهزتك وأجهزة أولادك وأسرتك محميةٌ منها. ستقوم هذه الخدمات بحجب هذه المواقع تلقائيًا ومنعها من العرض إذا طلبها متصفّح الويب الخاصّ بك أو بأحد أفراد أسرتك.

توجد هذه الإعدادات غالبًا في إعدادات اتصال الـDHCP الخاصّة بالموجّه:



إليك بعضًا من هذه المزوّدات (أدخلها في خانتيّ DNS Server وSecondary DNS Server) وهي قد تختلف من ناحية السرعة وقدرتها على حجب المواقع السيّئة، كما أنّ الأوّل والثالث أمريكيان بينما الثاني روسي (يمكنك تجربتهم واختيار ما تظنه الأسرع والأفضل):

- OpenDNS: 208.67.222.123, 208.67.220.123.
- Yandex DNS: 77.88.8.7, 77.88.8.3.
- CloudFlare Family: 1.1.1.1 (أدخل نفس العنوان في كلا الخانتين).

يحميك استخدام خدمة DNS خارجية من معرفة مواقع الويب التي تزورها من طرف المتطفّلين على اتصالاتك. هو ما يُعرف بثغرات "تسريب عناوين أسماء النطاقات" (DNS Leak). وهناك مواقع ويب لاختبار هذا التسريب مثل DNSLeakTest.com. تأكّد جيّدًا من استخدامك لمزوّد DNS خارجي فهو يحميك من عدّة مخاطر.

6. 4. خاتمة الفصل

صار هكذا كلٌ من حاسوبك والموجّه الخاصّ بك آمنين بصورة جيّدة وفقًا للتعليمات التي شرحناها. هناك المزيد من الأشياء التي يُمكنك فعلها بالطبع للحصول على المزيد من الخصوصية والأمان كاستخدام في بي إن، لكن يمكنك البحث عن هذه الأشياء بنفسك إن أردت على الشبكة أو سؤال المتخصصين في المجال عنها.

7. النسخ الاحتياطي

إنّ النسخ الاحتياطي عملية مهمّة جدًا لتأمين البيانات والملفّات لتجنّب فقدانها في حال حصول الأعطال أو سرقة الأجهزة أو غير ذلك من الظروف. سيشرح هذا الفصل كل الأساسيات المتعلّقة بالنسخ الاحتياطي وكيفية تأمين النُسَخ الاحتياطية وتخزينها واستخدامها.

7. 1. لماذا النسخ الاحتياطي مهم فوق ما تتصوّر

إنّ معظم المستخدمين لا يقومون بالنسخ الاحتياطي للأسف وبالتالي يتركون أنفسهم معرّضين لفواجع الزمان التي قد تحصل فجأة وتضيّع كلّ ذكرياتهم وبياناتهم وملفّاتهم المهمّة المخزّنة على تلك الأجهزة. ومن المهم امتلاك سياسة نسخ احتياطي قوية وفعّالة لتجنّب ذلك.

هناك العديد من السيناريوهات التي يصبح فيها النسخ الاحتياطي مهمًا جدًا سواءً لأجهزة الهاتف المحمول أو الحواسيب:

- توقّف الجهاز عن العمل فجأة وبالتالي تضيع كلّ الصور والملفّات والمستندات التي كانت عليه.
- تثبيتك لأحد البرمجيات الخبيثة عن طريق الخطأ على الجهاز أو وصول الفيروسات إليه وبالتالي تسببه في حذف ملفّاتك أو تشفيرها.
- سرقة الجهاز وبالتالي فقدان كلّ ما كان موجودًا عليه.
- تعديلك أو حذفك لأحد الملفّات المهمّة لك عن طريق الخطأ وبالتالي من المستحيل استرجاع النسخة القديمة دون النسخ الاحتياطي.

لكن هناك العديد من الطرق لإجراء النسخ الاحتياطي، فأيّها تختار؟

7. 2. أنواع النسخ الاحتياطي

تختلف أساليب النسخ الاحتياطي باختلاف أماكن تخزين النُسَخ الاحتياطية، وهناك نوعان رئيسيان لها:

- التخزين المحلّي (Local Storage): وهو ببساطة عمل نسخ احتياطية للملفّات المطلوبة ثمّ حفظها إمّا على أقراص صلبة متنقلة (Portable Hard-disk) أو فلاشات USB أو حفظها على وسائط شبيهة أخرى خارج نطاق شبكة الإنترنت.
- التخزين السحابي (Cloud Storage): وهو عملية تخزين الملفّات على خواديم أحد الشركات التي توفّر خدمات التخزين على الإنترنت (أو خادومك أنت)، مثل Google Drive وغيرها. وجاءت كلمة سحابة "Cloud" من كون ملفّات المستخدمين مخزّنة على خواديم بعيدة عنهم (مصطلح سحابة ما هو إلّا كناية عن كلمة الإنترنت في الواقع ولا يعني شيئًا خاصًا).

لكلٍ من هذين النوعين إيجابياته وسلبياته ونقاط القوّة والضعف الخاصّة به:

- يسمح التخزين المحلّي بنسخ ملفّاتٍ أكبر فأنت غير مقيّدٍ هنا بالمساحة المحدودة التي تعطيك إيّاها خدمة التخزين السحابي، وبالتالي يمكنك نسخ أشياء أكثر بل ونسخ بعض إعدادات النظام وبرامجه إن أردت، بل نسخ أقراص كاملة (مثل قرص C:/ أو D:/ على ويندوز) إن أردت ذلك.
- التخزين السحابي أسهل من التخزين المحلّي وهذا لأنّه مؤتمت (Automated) وكلّ ما عليك فعله هو حفظ ملفّاتك مباشرةً بدلًا من نسخها ولصقها يدويًا كما في التخزين المحلّي. أمّا في الأخير فعليك عمل النسخ الاحتياطي يدويًا بنفسك عند كل تغيير أو تحديث للملفّات بينما السحابي يلتقط التغييرات مباشرةً وتلقائيًا.
- التخزين المحلّي أأمن من ناحية أنّك غير مرتبط بخدمات شركة خارجية وبالتالي كلّ ملفّاتك موجودة تحت سيطرتك، بينما في التخزين السحابي ملفّاتك مرتبطة بالشركة ويمكنها أن تقطع عنك الخدمة لأي سبب. كما أنّك تضمن أنّه لا يمكن لأحدٍ الوصول لملفّاتك سواك فهي خارج نطاق الإنترنت.
- يمتلك التخزين السحابي مزايا متقدّمة مثل المزامنة مع مختلف الأجهزة (أندرويد وiOS وبقية أنظمة التشغيل) وبالتالي يمكنك الوصول إلى الملفّات على أيّ جهاز، بينما سيحتاج التخزين المحلّي الكثير من التعب للوصول إلى الملفّات على جهازٍ غير الجهاز الذي خُزّنت

عليه الملفّات. يوفّر التخزين السحابي مزايا أخرى مثل ميّزة مشاركة الملفّات مع أكثر من شخص تلقائيًا أو الاحتفاظ بأكثر من نسخة من نفس الملفّ.

يمكنك الآن اختيار أيّ نوعيّ التخزين ستستعمل وسنشرح طريقة العمل مع الاثنين.

7. 3. إجراء النسخ الاحتياطي مع التخزين السحابي

هناك العديد من التحديّات المتعلّقة بالتخزين السحابي بالفعل مثل أمان وخصوصية ملفّاتك المخزّنة عليه؛ فالتخزين السحابي في النهاية هو تخزينٌ لملفّاتك المهمّة على خواديم شركاتٍ أجنبية بعيدة عنك، لكن من الممكن استعماله بأمان إن اتبعت الطرق المناسبة لتأمين ملفّاتك.

ستحتاج أن تشترك أوّلًا في أحد خدمات التخزين السحابي، وبعدها يمكنك البحث عمّا يسمّى بالتكاملات (Integrations) بين نظام تشغيلك الحالي وبين خدمة التخزين السحابية تلك؛ وهي التطبيقات التابعة لتلك الخدمة والتي عليك تثبيتها على نظامك لاستخدام خدمة التخزين السحابي بدلًا من الاعتماد على واجهة الويب داخل المتصفّح طوال الوقت. حيث ستقوم هذه التكاملات تلقائيًا بنسخ وتخزين ومزامنة ملفّاتك الموضوعة فيها بدلًا من حاجتك لقيامك بذلك يدويًا. إنّ خدمات التخزين السحابي قادرة على مزامنة ملفّاتك بين مختلف الأجهزة التي تستعملها (حواسيب وهواتف محمولة) بسبب ذلك.

إليك أوّلًا بعض خدمات التخزين السحابي المعروفة:

- Dropbox: شركة أمريكية توفّر خدمة تخزين سحابي مجانية بحجم 2 جيجابت للمستخدمين، كما توفّر بعض المزايا المتقدّمة مثل المشاركة الجماعية ودعم للهواتف المحمولة (iOS, أندرويد) وغير ذلك.
- Google Drive: خدمة تخزين سحابي مجانية بحجم 15 جيجابت من شركة جوجل.
- ProtonDrive: خدمة سويسرية تابعة لشركة ProtonMail التي ذكرناها في فصولٍ سابقة من هذا الكتاب، وميّزة هذه الخدمة مقارنةً بالخدمات الأخرى أنّها تستعمل تشفير طرف لطرف (End-to-End Encryption) للملفّات المخزّنة عليها افتراضيًا وبالتالي لا يمكن لأحدٍ سواك الوصول إلى ملفّاتك. لكنّها مدفوعة للأسف وليست مجانية إلّا أنّها أفضل الموجود بالسوق لمن يريد أقصى حماية [1]. ما تزال لم تصدر بعد في تاريخ إصدار هذا الكتاب لكن ستصدر قريبًا ويمكنك متابعتها.

اشترك في واحدةٍ من هذه الخدمات ثمّ ثبّت التطبيقات المتوافقة مع نظام تشغيلك الحالي

الخاصّة بها. ستجد بعدها أنّ التطبيق يزوّدك بمجلّد مزامنة خاصّ لوضع ملفّاتك التي تريد مزامنتها تلقائيًا عبر الخدمة (مثلًا مجلّد اسمه Dropbox في المسار /home/username/ على أنظمة لينكس مع خدمة دروب بوكس). هذا المجلّد هو في الواقع خزنتك الكاملة على تلك الخدمة فكلّ تعديل تجريه عليها من إضافة وإزالة ملفّات سيصبح تلقائيًا موجودًا على كلّ أجهزتك الأخرى.

الآن بدلًا من أن تخزّن ملفّاتك محليًّا على جهازك (الصور، الفيديوهات، المستندات... إلخ) استعمل هذه المساحة المخصصة لك لتخزينها. فقط احفظ الملفّات داخل مجلّد المزامنة بدلًا من حفظها في مجلّدات النظام العادية.

بالنسبة للهواتف المحمولة فإن كنت تستعمل نظام أندرويد فهناك خياراتٌ كثيرة لمزامنة الصور مثلًا مع خدمة Google Drive تلقائيًا من إعدادات تطبيق الصور، ويمكنك فعل نفس الأمر على نظام iOS مع خدمة iCloud من شركة آبل نفسها.

تأكّد دومًا أنّ جميع ملفّاتك المهمّة موجودة على خدمة التخزين السحابي، ويمكنك استخدام أكثر من خدمة في نفس الوقت كذلك لضمان عدم ضياع ملفّاتك إن اختفت واحدةٌ منها فجأة.

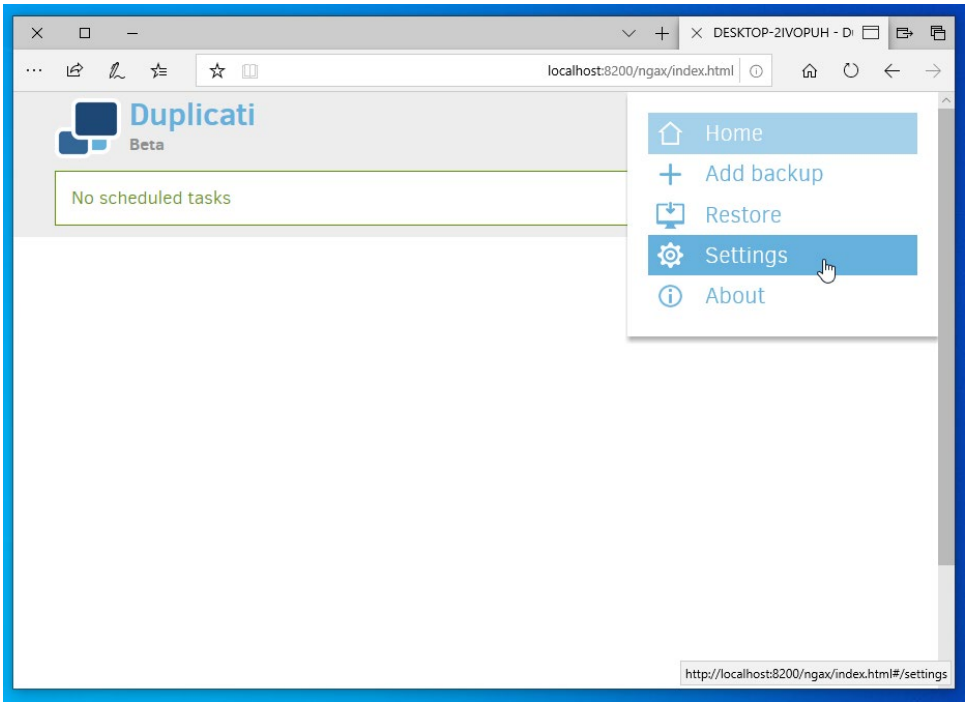
7. 4. إجراء النسخ الاحتياطي مع التخزين المحلّي

يمكنك كذلك أن تجري عمليات النسخ الاحتياطي محليًا دون الحاجة للاعتماد على خدمات شركاتٍ خارجية، بل فقط عبر استعمال التخزين المحلّي (Local Storage) كالأقراص الصلبة الخارجية أو فلاشات USB أو غير ذلك من الوسائط التي تريدها.

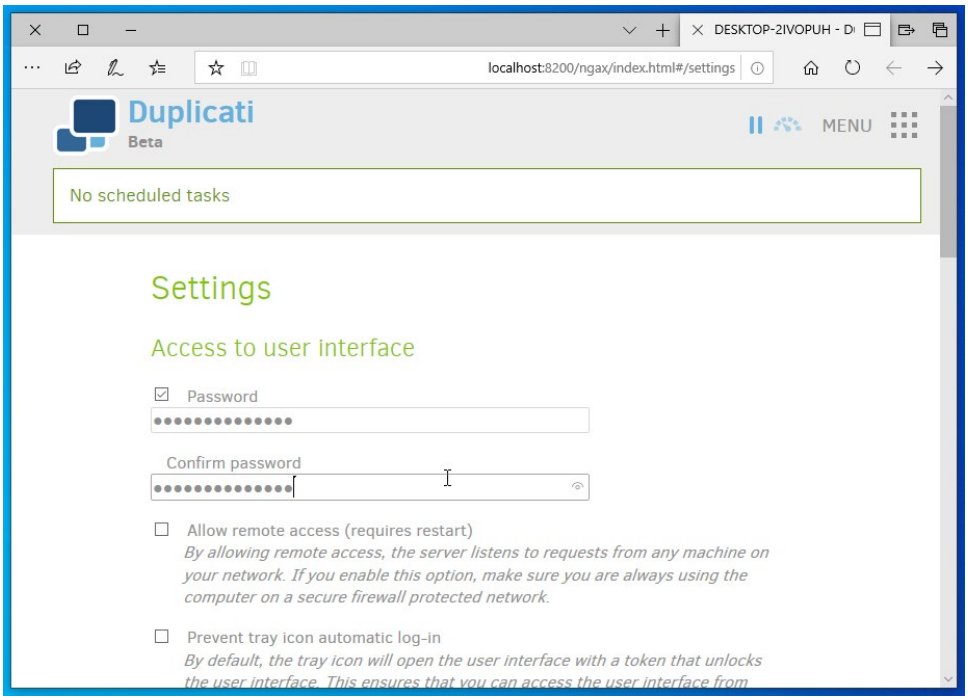
لاحظ أنّه عليك تخزين الملفّات في مكانٍ غير المكان الذي نسخت منه البيانات؛ إذا كنت تريد نسخ ملفّات حاسوبك المهمّة فلا تضغطها مثلًا في ملفّ ثمّ تخزّنها على نفس الحاسوب، بل عليك وضعها على فلاشة USB مستقلة أو قرص صلب منفصل أو ما شابه ذلك، وينطبق نفس الأمر على الهاتف المحمول، وهذا لأنّه في حال حصول مشكلة كبيرة لذاك الجهاز فستضيع النسخة الاحتياطية معه كذلك (سرقة، اختراق، فيروس ...إلخ).

من البرامج الجيّدة لعمل النسخ الاحتياطي برنامج يدعى "Duplicati" وهو برنامج مجاني ومفتوح المصدر ويعمل على ويندوز وماك ولينكس. يمكنك تحميله من موقعه الرسمي ثمّ تثبيته في أقل من دقيقة. واجهة التطبيق هي واجهة ويب (أي أنّ البرنامج سيعمل من داخل متصفّح الويب) كما أنّه يستعمل التشفير افتراضيًا للنُسَخ الاحتياطية ويدعم الجدولة لأتمتة النسخ الاحتياطي بدلًا من القيام به يدويًا، وغير ذلك من المزايا.

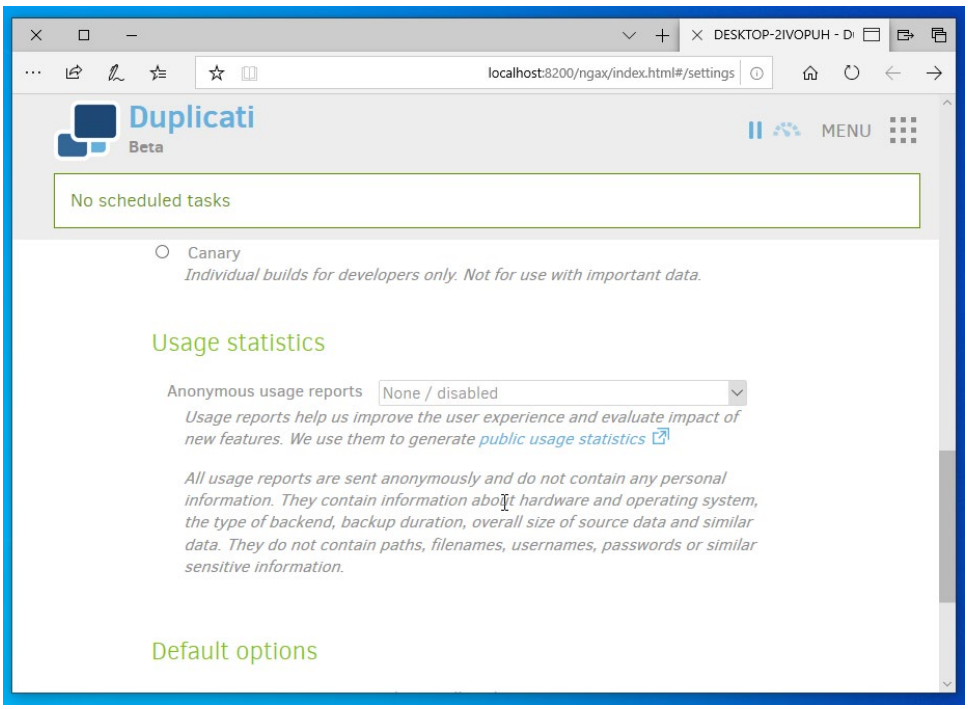
علينا أوّلًا تأمين البرنامج بعد تثبيته، وهذا عبر إنشاء كلمة مرور للوحة التحكّم الخاصّة به. اذهب إلى Settings كما في الصورة:



ثمّ أدخل كلمة مرور قوية لاستخدامها للوحة تحكّم البرنامج:

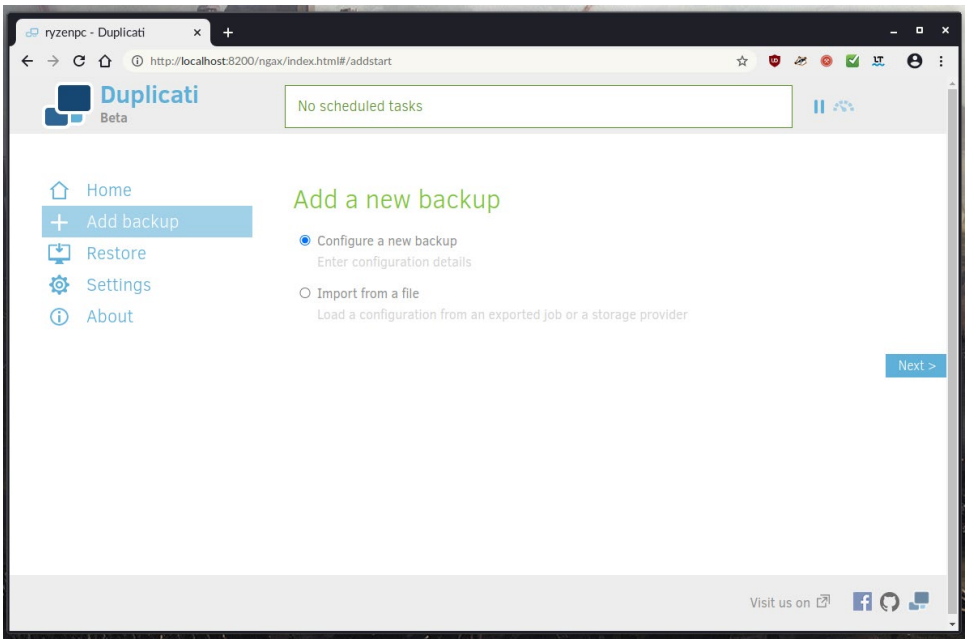


ويمكنك تعطيل خيارات إرسال البيانات كذلك لتجنّب إرسال أيّ شيء عن جهازك إلى الشركة المطوّرة:

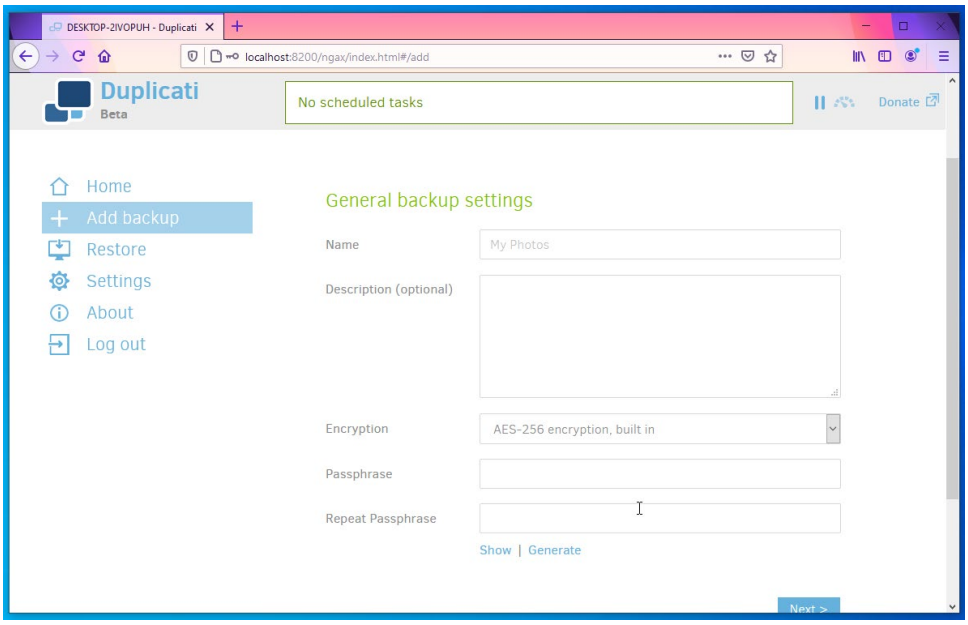


سيطلب منك البرنامج الآن إدخال كلمة المرور الجديدة.

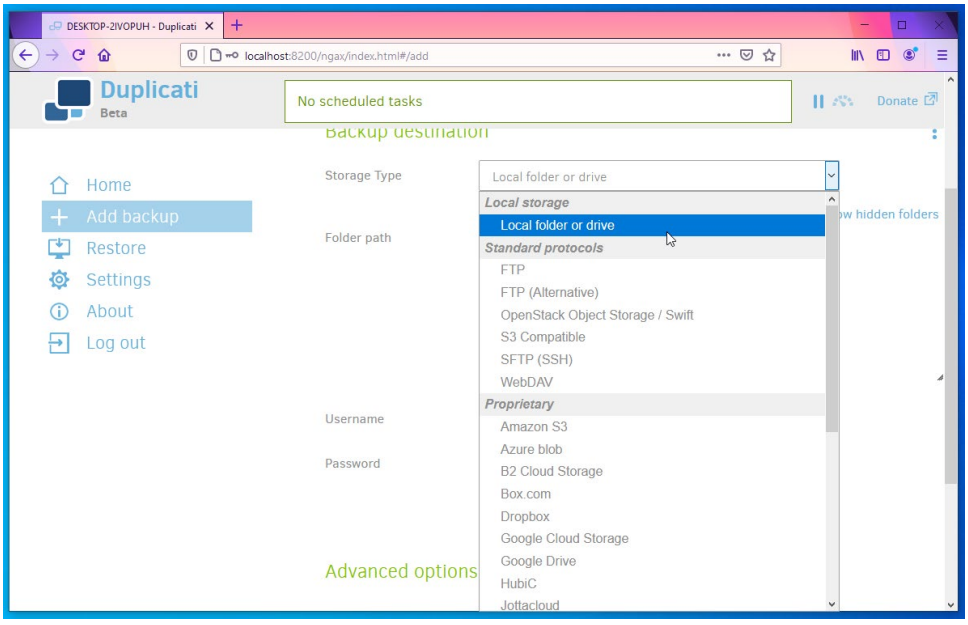
يمكنك الآن البدء بإجراء عملية النسخ الاحتياطي. اذهب إلى الواجهة الرئيسية واضغط على "Add Backup" من القائمة النقطية. ثمّ اختر "Configure a new Backup":



يمكنك الآن كتابة اسم النسخة الاحتياطية ووصفها، بالإضافة إلى تعيين كلمة مرور قوية لها (دع خيار نوع التشفير على ما هو عليه). لا تنس أنّه عليك استخدام كلمة مرور قوية وآمنة لأنّها ستُستعمل في تشفير نسخك الاحتياطية كذلك، كما لا تنسى أنّه عليك تذكّرها أو حفظها:

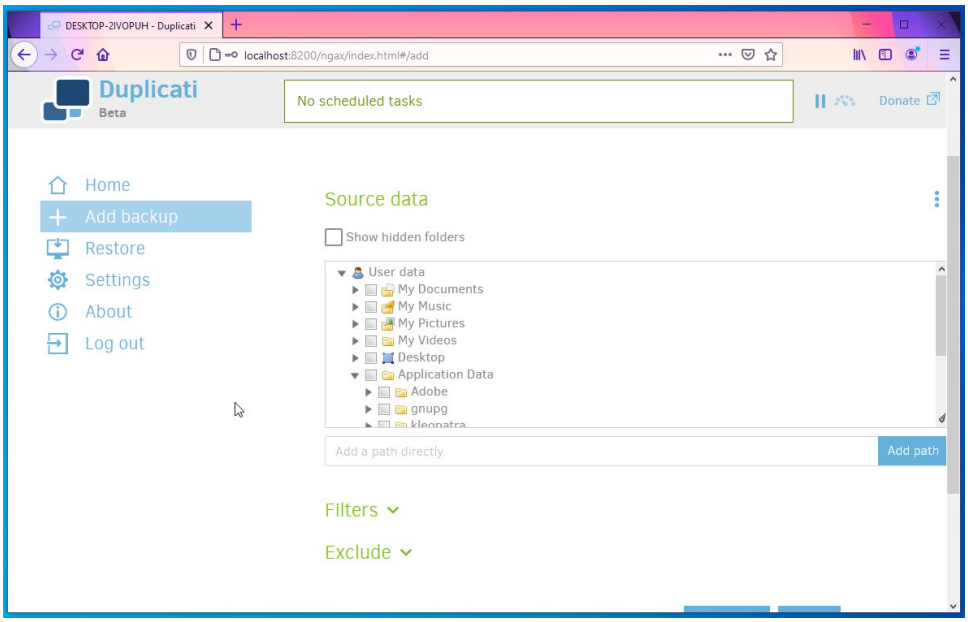


سيخيّرك البرنامج بعدها عن مكان تخزين النسخ الاحتياطية؛ فيمكنك مثلًا تخزينها على أحد مجلّدات النظام نفسه (Local folder or Drive) أو يمكنك تخزينها على الإنترنت عبر الخيارات الأخرى المتوفّرة كذلك مثل FTP أو خدمات شركات التخزين السحابي كـDropbox وGoogle Drive وغيرها:

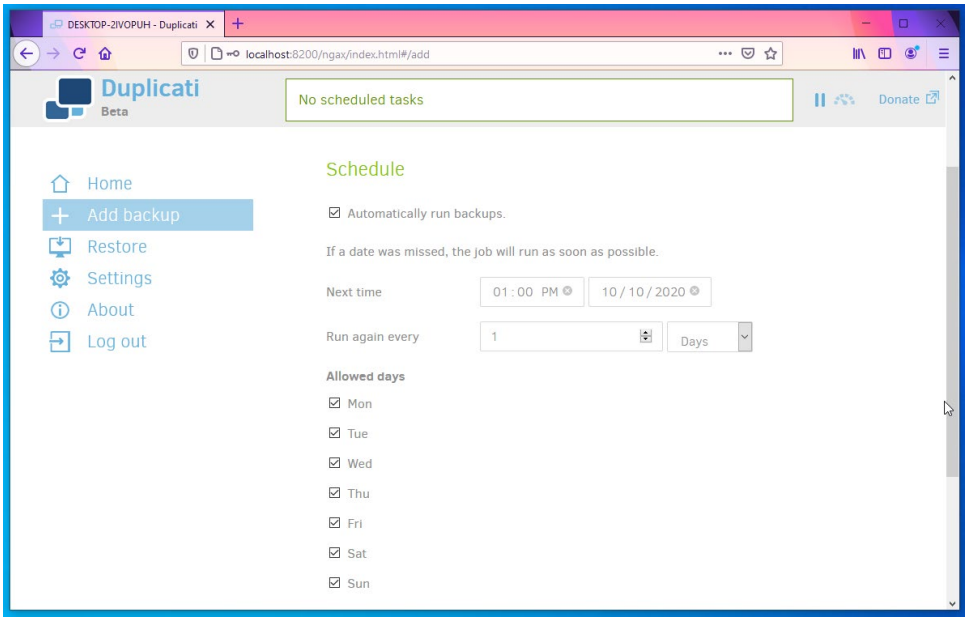


السيناريو المثالي لتخزين النسخ الاحتياطية محلّيًا هو أن تصل قرصًا صلبًا محمولًا (Portable Hard-disk) أو فلاشة USB طوال الوقت مع الجهاز لتستعملها للنسخ الاحتياطي بصورة مستمرة. يمكنك أن تختار القرص أو الفلاشة من نفس الصفحة بعد وصلهما للجهاز.

سيطلب منك البرنامج الآن تحديد الملفّات والبيانات المطلوب نسخها. يمكنك نسخ إعدادات تطبيقاتك الحالية عبر تعليم "Application Data"، ويمكنك كذلك اختيار بعضٍ منها دون أن تختارها جميعًا. يمكنك كذلك اختيار ملفّات أو مجلّدات أو أقراص معيّنة تريدها:

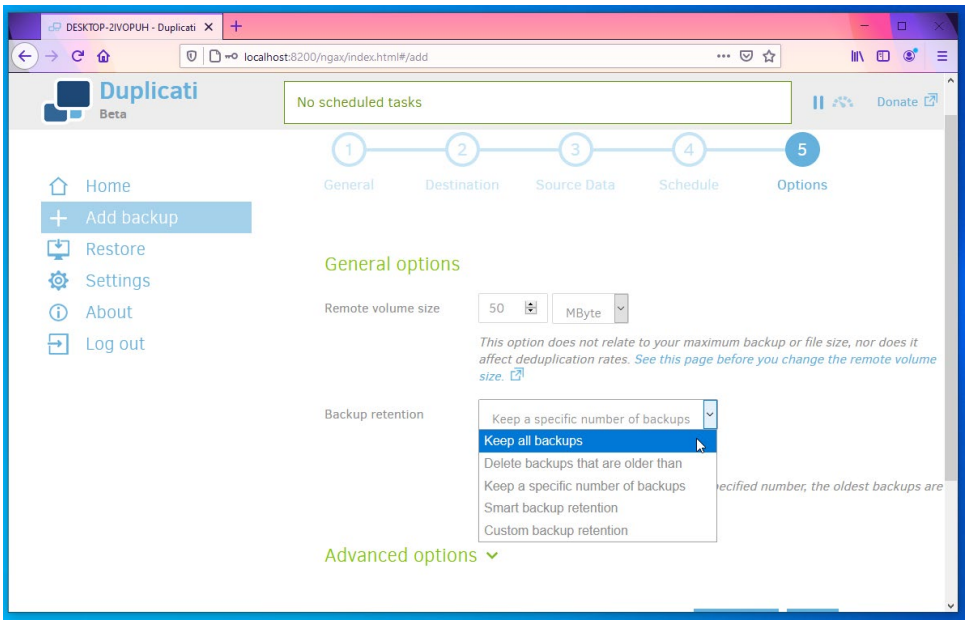


ستأتيك بعدها إعدادات الجدولة؛ حيث يدعم البرنامج تشغيل عملية النسخ الاحتياطي تلقائيًا في أوقات تحددها أنت بدلًا من قيامك بذلك يدويًا. اختر الأوقات التي تناسبك (ننصح بألّا تقل عن نسخة احتياطية واحدة بالأسبوع):



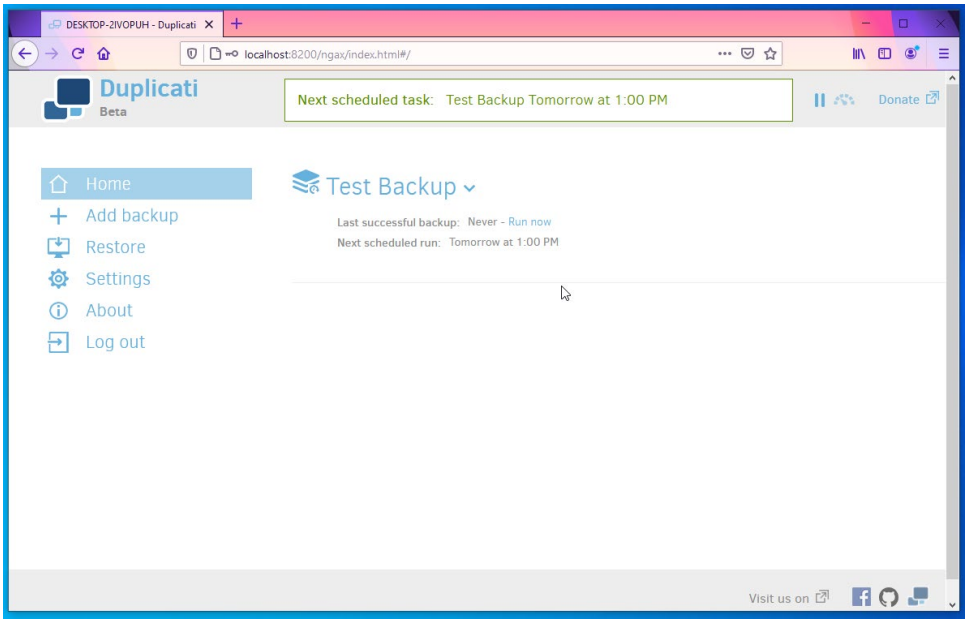
ستأتيك أخيرًا بعض الخيارات المتعلّقة بالنُسَخ الاحتياطية وعددها. يمكنك الاحتفاظ بجميع النسخ الاحتياطية (Keep all backups) أو حذف النسخ الاحتياطية الأقدم من عمرٍ معيّن (Delete

backups the are older than) أو الإبقاء على عددٍ معيّن من النسخ الاحتياطية الأحدث (Keep a specific number of backups):



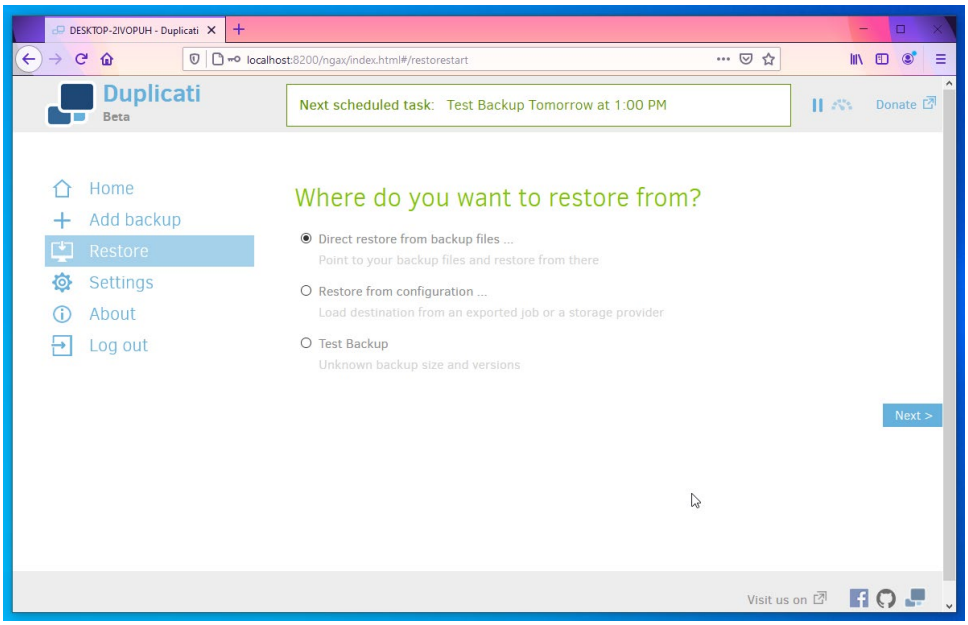
ننصح باختيار خيار الإبقاء على عددٍ معيّن من النسخ الاحتياطية ثم كتابة العدد الذي يناسبك (الإبقاء على أحدث 6 أو 7 نسخ احتياطية مثلًا، بناءً على حجم بياناتك والمساحة المتوفّرة في وسيط التخزين الذي تخطط لاستخدامه.

ستجد بعدها أنّ النسخة الاحتياطية قد أُنشِئت:



جرّب الضغط على "Backup Now" ومن المفترض أن تتم عملية النسخ الاحتياطي بنجاح دون أن تواجه مشكلة.

إذا حصلت معك مشكلة في الجهاز مستقبلًا وضاعت ملفّاتك فيمكنك إعادة تثبيت البرنامج من جديد ثمّ الذهاب إلى تبويب "Restore" واختيار مسار النسخة الاحتياطية لبدأ عملية الاستعادة منها:



هذه هي كلّ العملية.

7. 5. خاتمة الفصل

صارت ملفّاتنا آمنة الآن بصورة مستمرة بفضل استخدام النسخ الاحتياطي، لكننا سنحتاج استخدام التشفير إن استخدمنا التخزين السحابي (والمزيد عن ذلك في الفصل القادم) لحماية ملفّاتنا من المتطفلين ومن شركات التخزين نفسها.

عدا عن ذلك بياناتنا آمنة الآن ويمكننا استرجاع ما نشاء منها في أيّ وقتٍ نريده.

8. التشفير واستعمالاته

سيشرح هذا الفصل بعض الاستخدامات الأساسية للتشفير وكيف يمكنه المساهمة بحماية بياناتك التي تريد نقلها عبر الشبكة إلى أماكن أخرى. هناك مواضيع متفرقة عن التشفير في مختلف أجزاء هذا الكتاب لطبيعة كون التشفير تقنيةً مستخدمة في الكثير من تقنيات علوم الحاسوب، لكننا سنشرح هنا بعض الأساليب التي تعتمد على التشفير بصورة أساسية.

8.1. مفاتيح التشفير

هناك الكثير من العلوم الفرعية المنضوية تحت مبدأ التشفير، لكننا نريد الحديث الآن عمّا يعرف بالمفاتيح (Keys).

هناك حاجة ملحّة للكثير من الناس لتشفير الرسائل والملفّات المتبادلة بينهم مثلًا، لكنهم بحاجة إلى طريقةً تسمح للمُرسِل أن يُرسل البيانات المشفّرة إلى المتلقّي ويتمكّن المتلقّي وحده فقط من إلغاء تشفيرها للوصول إلى البيانات الحقيقية. وهذه مشكلة على الإنترنت لأنّ البيانات تمرّ عبر مزوّد خدمة الإنترنت (ISP) وقد ترفعها مثلًا على خدمات شركات مثل جوجل وواتساب وفيس بوك وغيرها، وبالتالي قد تطّلع عليها أكثر من جهة، ولهذا لا نريد مثلًا إرسال كلمة مرور كلّ مرّة مع الملفّ المشفّر للمتلقّي لأنّ هذا يعني أنّ كل الأطراف المتمكنة من الشبكة سيكون لها وصولٌ كذلك إلى محتويات الملفّ (فهي لديها وصول إلى كلمة المرور كذلك).

نشأت بسبب هذه الحاجة ما تعرف بمفاتيح التشفير الشخصية، وهما زوجان من المفاتيح المرتبطة ببعضها، واحدٌ منهما يسمّى المفتاح العام (Public Key) والثاني هو المفتاح الخاصّ (Private Key) وهما مرتبطان ببعضهما البعض دونًا عن غيرهما من المفاتيح. يمكن للمرء أن يمتلك العديد من المفاتيح إن أراد.

بفضل علم التعمية (Cryptography) ومبادئ التشفير القائمة على رياضياتٍ دقيقة فإنّه يمكن لأيّ شخص أن يقوم بتشفير رسالة إلكترونية مثلًا وفق المفتاح العام لشخصٍ معيّن، لكن لا يمكن سوى للشخص الذي يمتلك المفتاح الخاصّ المرتبط بذاك المفتاح العام أن يقوم بإلغاء تشفير تلك الرسالة. وبالتالي إذا أراد أحدهم مراسلتك مثلًا برسالة بريدية مشفّرة، فكل ما عليه فعله هو البحث عن مفتاحك العام على الشبكة (حيث أنّه منشور للكل على عكس المفتاح الخاصّ) واستخدامه لتشفير الرسالة ثمّ إرسالها إليك، ببساطة. وستتمكن أنت فقط من إلغاء تشفير الرسالة عبر مفتاحك الخاصّ الشخصي بك والمرتبط بالمفتاح العام الذي شُفّرت الرسالة به.

وللمزيد من الحماية، فإنّ مفتاحك الخاصّ محمي بكلمة مرور تحددها أنت وبالتالي لا يمكن حتّى مع امتلاك المفتاح الخاصّ من طرف الآخرين أن يستخدموه ضدّك ليكسروا تشفير ملفّاتك ورسائلك (ولكن بالطبع هذا لا يعني أنّه يمكنك مشاركة المفتاح الخاصّ مع الناس لأنّه هناك طرق لكسر كلمات المرور مثل القوّة الغاشمة Bruteforce التي شرحناها مسبقًا وغيرها). ومن المهم أن تحتفظ بكلمة المرور هذه وتتذكّرها طوال الوقت، كما من المهم أن تكون كلمة مرورٍ قوية كما سنشرح في فصل "كلمات المرور" في هذا الكتاب. وهذا لأنّك ستحتاج كلمة المرور في كلّ مرّة تريد فيها استخدام المفاتيح. إن فقدت كلمة المرور فحينها ستفقد كلّ بياناتك المشفّرة ولن تتمكن من استرجاعها.

والآن لن تتمكن أيّ جهة بما فيها مزوّد خدمة الإنترنت أو الشركة الموفّرة للمنصّة الإلكترونية ولا أي طرف آخر سواك أنت (والمُرسِل بالطبع) من معرفة محتوى الرسائل والملفّات عبر هذه الطريقة، لأنّك أنت فقط من يمتلك المفتاح الخاصّ (تذكّر أنّ المفتاح الخاصّ لا يُشارك مع أي شخصٍ آخر بتاتًا ولا حتّى المُرسِل).

تُستخدم مفاتيح التشفير في الكثير من الأنظمة المختلفة في علوم الحاسوب وهي من أبرز الطُرق لحماية البيانات، وتستخدمها الكثير من البرامج لتشفير الملفّات أو الرسائل الإلكترونية أو البيانات الأخرى بصورة عامّة.

وتُستخدم هذه المفاتيح الشخصية لأكثر من التشفير، فيُمكن استخدامها من أجل ما يسمّى بالتوقيع الرقمي (Digital Signature)، وهو كما التوقيع الحقيقي للإنسان، ضمانٌ أنّ الملفّ أو الرسالة الإلكترونية هي من طرف ذاك الشخص بالفعل لكن دون تشفير الملفّ أو الرسالة. وهذا مهم لأنّه في الكثير من الأحيان قد يحتاج الناس لطريقةٍ لضمان موثوقية هذه الملفّات لكن لا يريدون تشفيرها. فيمكن أن تحاول بعض الجهات انتحال شخصية مستخدمٍ ما مثلًا ولن يكون لديك ضمانٌ من أنّ الملفّ الذي حمّلته هو من ذاك الشخص بالفعل وليس من طرفٍ مشبوه ينتحل شخصيته (مثل

تحميل أحد توزيعات لينكس، قد يقوم أحد المخترقين باختراق موقع التوزيعة ووضع رابط تحميل لملفّ خبيث بدلًا من التوزيعة الأصلية ولن تتمكن من معرفة ذلك دون أن تتحقق من التوقيع الرقمي للملفّ، ومعظم المستخدمين لا يقومون بذلك للأسف).

هناك بالطبع معايير مختلفة (Standards) لطريقة بناء هذه المفاتيح وتشفيرها ومشاركتها وتخزينها، أبرزها هو المبدأ المفتوح OpenPGP. وهنالك العديد من المكتبات البرمجية (Software Libraries) التي توفّر أدوات التشفير الحقيقية لتشفير البيانات والملفّات وفق تلك المعايير، أبرزها GnuPG وهي مكتبة حرّة ومجانية ومفتوحة المصدر ومن أكثر المكتبات استخدامًا على الإطلاق في مجال الأمان الرقمي.

يُمكنك إنشاء مفاتيح التشفير الخاصّة بك (المفتاح العام والخاصّ) من داخل نظام التشغيل الحالي الذي تستعمله، ولهذا تختلف الطريقة بناءً على ذلك النظام. يمكنك إنشاء زوجيّ المفاتيح على نظام لينكس وmacOS عبر الأمر التالي:

```
gpg --full-generate-key
```

سيسألك برنامج gpg بضعة أسئلة مثل:

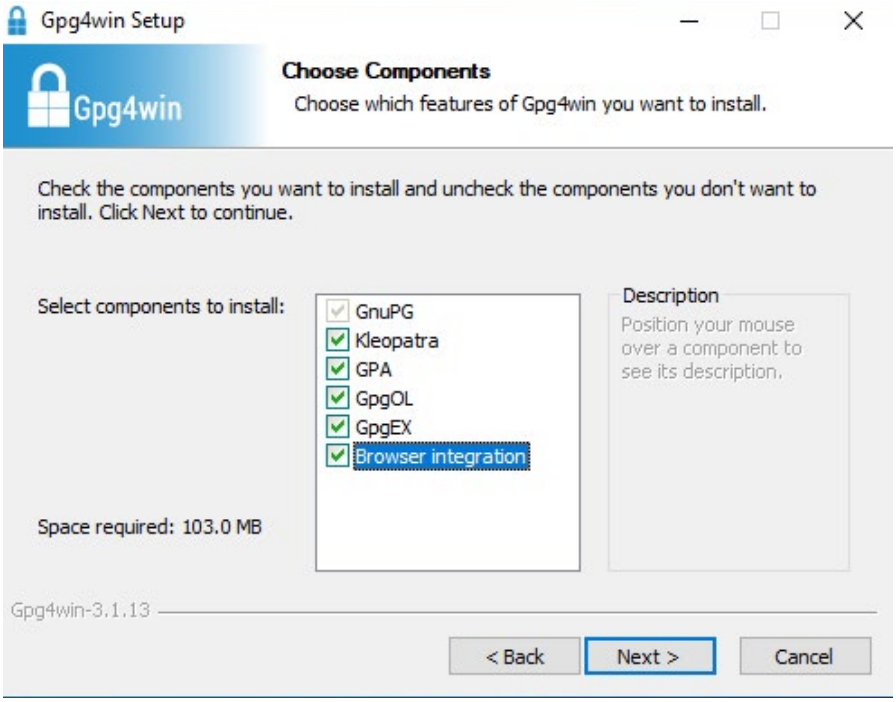
- نوع خوارزمية التشفير المُرادة، مثل RSA أو DSA وغيرها. الخيار الافتراضي هو "RSA and RSA" وكلّ ما عليك فعله هو الضغط على Enter للمتابعة.
- طول مفتاح التشفير المُراد. لا حاجة للتفكير الطويل هنا بل فقط اختر الإعدادات الافتراضية حاليًا (3072) واضغط Enter.
- مدّة صلاحية المفتاح. هل تريد أن تنفذ صلاحية هذا المفتاح بعد وقتٍ معيّن، وبالتالي كلّ شيءٍ شُفّر أو وُقّع عبره لن يكون قابلًا للتأكّد من صحّته أو إلغاء تشفيره بعد انتهاء الوقت المعيّن؟ إن كان الجواب لا، فحينها اضغط Enter (الخيار الافتراضي) لجعل المفتاح غير محدود الصلاحية.
- قد يطلب منك gpg تأكيدًا للخطوة السابقة. اكتب y (اختصارًا لـyes).
- سيسألك gpg كذلك عن اسمك وبريدك وتعليقٍ قصير حول المفتاح.
- سيعرض لك gpg معلومات المفتاح بصورتها النهائية. إن لم يكن لديك تغيير تريد إجراءه فحينها اكتب O (اختصارًا لـOkay).
- أخيرًا، سيُطلب منك إدخال كلمة مرورٍ لحماية مفاتيح التشفير.

ستجد المفتاح العام والمفتاح الخاصّ في ملفّين منفصلين في المسار gnupg. داخل مجلّد المنزل الخاصّ بك. تذكّر أنّه يجب ألّا تشارك المفتاح الخاصّ مع أي شخصٍ بتاتًا، كما تذكّر أنّه عليك حفظه في مكانٍ آمن لا يصل إليه أحدٌ سواك، هو وكلمة المرور (يمكنك مثلًا وضعهم داخل فلاشة USB ورميها في مكانٍ آمن في منزلك).

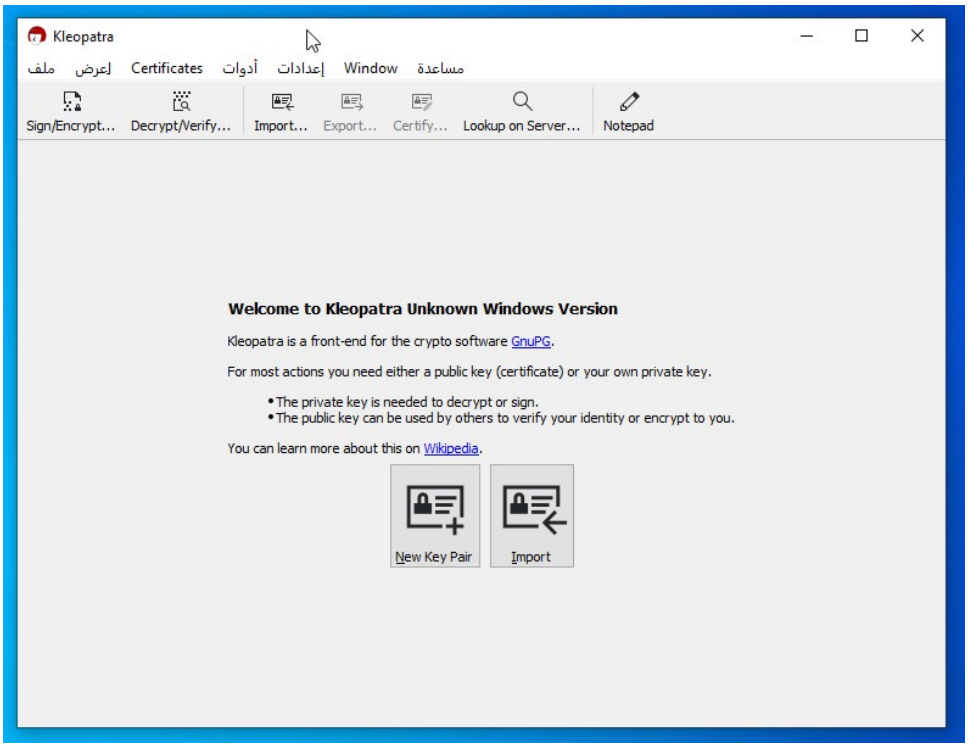
نستحسن ألّا تحاول العبث بالملفّات داخل مجلّد gnupg. بنفسك، لكن يمكنك تصدير المفاتيح وإدارتها واستيرادها عبر الأمر gpg نفسه من سطر الأوامر. ويمكنك البحث عنه على الإنترنت للمزيد من المعلومات أو رؤية التوثيق الكامل له عبر:

```
gpg --help
```

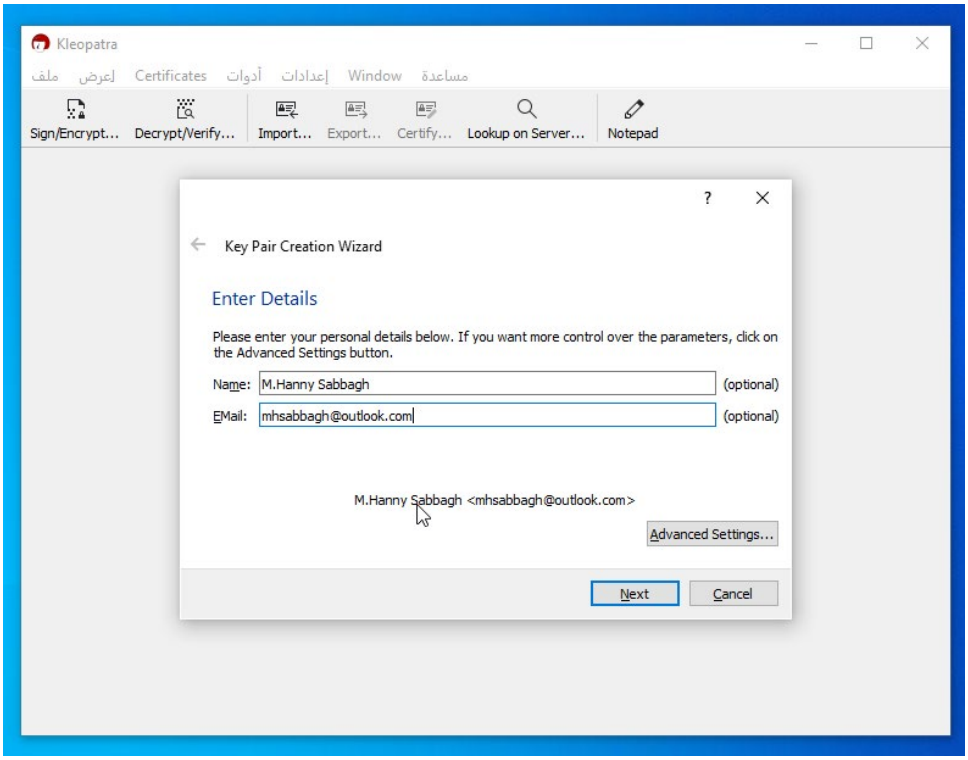
أمّا بالنسبة لأنظمة ويندوز، فالعملية سهلة بفضل برنامج Gpg4Win، وهو برنامجٌ مفتوح المصدر ومجاني. كلّ ما عليك فعله هو تحميل البرنامج وتثبيته. تأكّد من تفعيلك للخيارات التالية أثناء تثبيته:



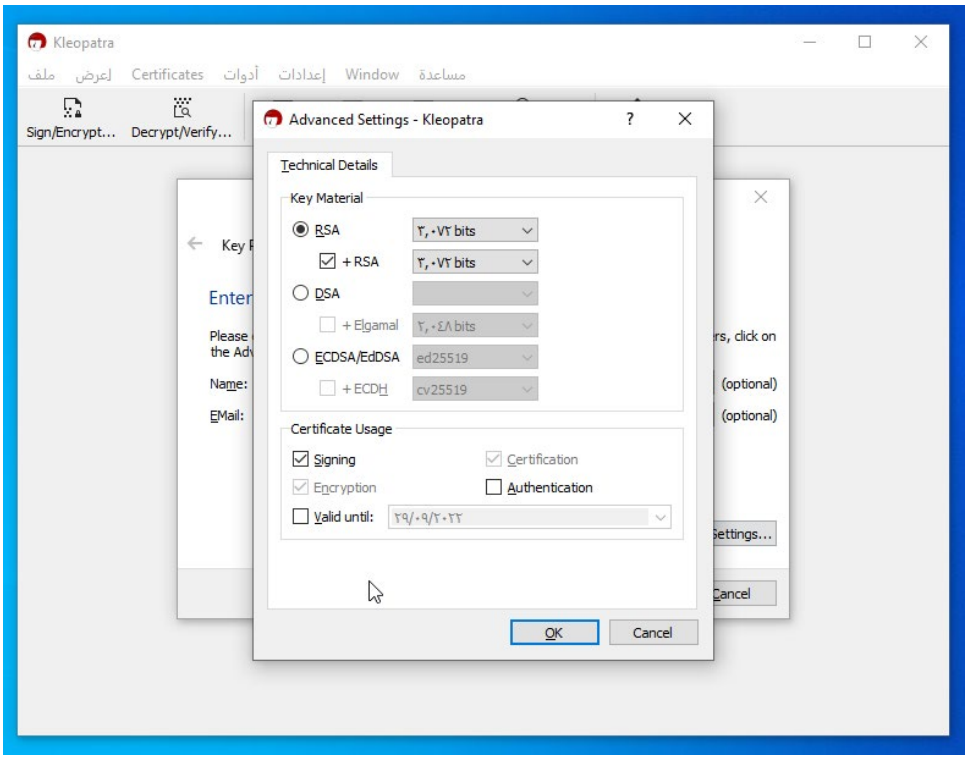
ستجد برنامجًا اسمه Kelopatra على نظامك بعد التثبيت، وهو الواجهة الرسومية لمكتبة GnuPG على أنظمة ويندوز. اضغط على "New Key Pair" كما في الصورة لإنشاء زوجيّ مفاتيح جديدة:



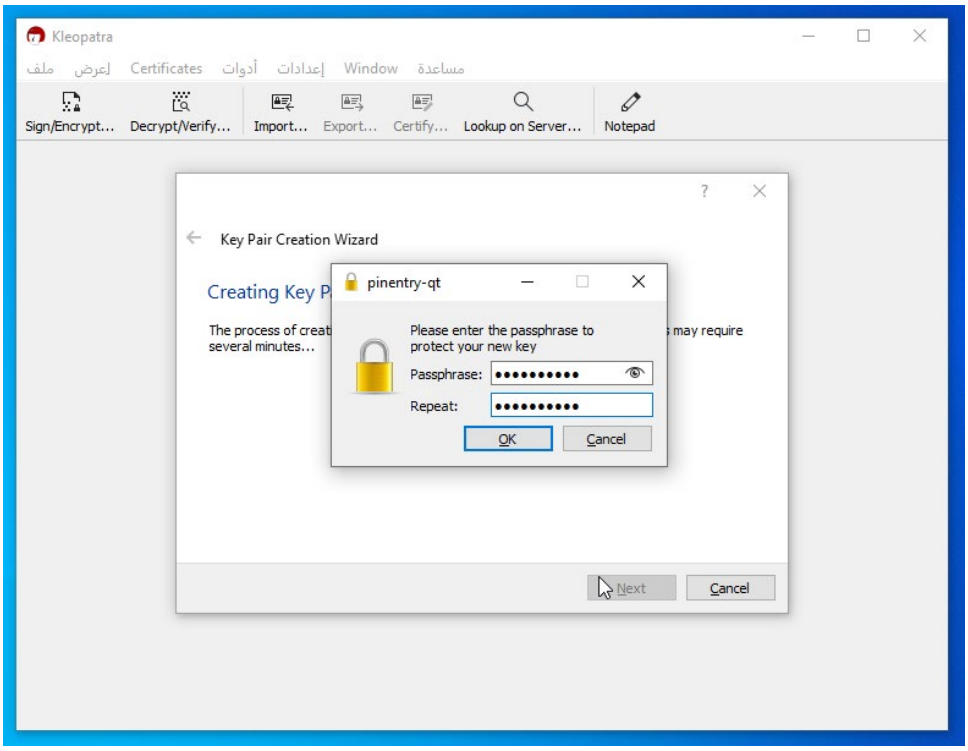
ثمّ أدخل اسمك وبريدك الإلكتروني:



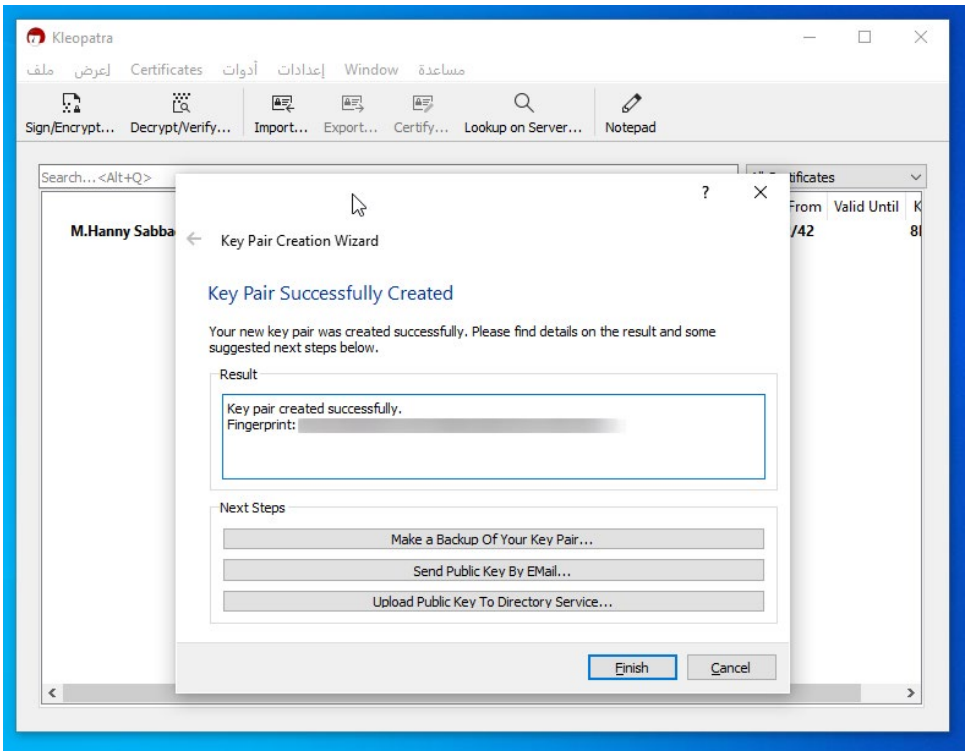
واضغط كذلك على "Advanced Settings". ستصل بعدها إلى النافذة التالية، أزل علامة صح من جانب "Valid until" لكي تجعل المفتاح بلا تاريخ صلاحية محدد (لا ينتهي):



وأخيرًا، أدخل كلمة المرور التي تريدها:



وهذه هي العملية ببساطة! يمكنك الآن تصدير المفاتيح أو حفظها أو عمل ما تشاء بها.



يُمكنك استخدام المفتاحين لاستقبال وإرسال البيانات المشفّرة بمجرّد أن تنشئهما مع مختلف البرامج والأدوات. يمكنك إنشاء عدة مفاتيح كذلك بناءً على كلّ نوع من الاستخدامات التي تريدها (مثلًا واحد للرسائل الإلكترونية والآخر للملفّات المشفّرة ...إلخ).

8. 2. تبادل رسائل البريد الإلكتروني المشفرة والموقعة

تدعم معظم خدمات البريد الإلكتروني تشفير الرسائل البريدية بين المستخدمين. لكن لتبادل الرسائل الإلكترونية بينك وبين مستخدمٍ آخر فعليكما أنتما الاثنان أن تمتلكا المفاتيح العامّة (Public Keys) الخاصّة بالآخر، وهذا لتشفير الرسائل بصيغةٍ تمكّن الطرف الآخر وحده من فكّ تشفيرها. يمكنكما تبادل المفاتيح العامّة عبر أي وسيلة اتصال أو حتّى نشرها على الإنترنت بأريحية.

تختلف طريقة إعدادها بناءً على الخدمة التي تستعملها، لكن بصورة عامّة، عليك تثبيت ما يُعرف ببرنامج بريد الإلكتروني المحلّي (Email Client) على جهازك، ثمّ ربطه بخدمة البريد الإلكتروني التي تستعملها، ثمّ تفعيل ميّزة تشفير الرسائل وإضافة مفاتيحك العامّة والخاصّة إلى البرنامج ليستخدمها.

وبما أنّه هناك العشرات من خدمات البريد الإلكتروني المختلفة بالإضافة إلى العشرات من البرامج المحلّية لإدارة البريد الإلكتروني وعلى مختلف أنظمة التشغيل، فإننا لن نشرح العملية بالتفصيل في هذا الكتاب ونترك المُستخدم ليختار خدمته وبرنامجه اللذين يناسبانه.

لكننا نُشير إلى بضعة أمور:

- حتّى مع استخدام التشفير فإنّه ما يزال بإمكان مزوّد خدمة البريد الإلكتروني، و(ربّما) مزوّد خدمة الإنترنت بالإضافة إلى أطرافٍ ثالثة (3rd-party) أن تعرف عنوان الرسائل الإلكترونية، بالإضافة إلى العنوان المُرسِل والعنوان المُستقبِل. أي أنّ التشفير لا يشمل هذه الحقول الثلاثة، ولذلك لا تضع شيئًا مهمًا فيها واعلم أنّ الغير قد يطّلعون عليها.
- لا تستخدم معظم - إن لم يكن كلّ - برامج إدارة البريد الإلكتروني المحلّية التشفير بصورة افتراضية؛ أيّ أنّ إضافة المفاتيح واستيرادها إلى البرنامج لا يكفي. عليك التأكّد بالضبط أنّ الرسالة الحالية التي تريد إرسالها ستكون مشفّرة. قد يكون في بعض البرامج خياراتٌ لتشفير كلّ الرسائل افتراضيًا، لكن عليك التحقق من ذلك بنفسك. وبالطبع، عليك إضافة المفاتيح العامّة للشخص الذي تُريد مُراسلته قبل التمكّن من إرسال رسالة بريدية مشفّرة إليه (سيقوم هو بتصديرها لك ثمّ تقوم أنت باستيرادها من داخل البرنامج أو النظام، وكذا بالنسبة لك).
- يُمكنك توقيع الرسالة رقميًا (Digital Signing) بنفسك وعبر مفتاحك الخاصّ دون الحاجة لشيءٍ من أحد، لكن من أجل التشفير فعليك امتلاك المفتاح العامّ للطرف الآخر وعليه أن يمتلك هو كذلك مفتاحك العام.
- هل يجب عليك تشفير كلّ الرسائل أم فقط الحساسة والمهمّة منها؟ يعتمد هذا على مدى درجة عامل الخطورة (Threat Factor) الذي أنت محاطٌ به، وإلى أيّ مدىٍ تريد تأمين نفسك وضدّ من.

بخصوص رسائل البريد الإلكتروني الموقّعة فالمفترض أنّ البرنامج الذي تستعمله سيعرض لك في "ترويسة الرسالة" (Message Headers) ما إذا كانت موقّعة بصورة صحيحة وموثوقة من الطرف الآخر الذي استقبلتَ الرسالة منه أم لا.

8. 3. تبادل الملفّات المشفّرة

يُمكنك تشفير الملفّات وتبادلها مع الآخرين باستخدام المفاتيح العامّة والخاصّة تمامًا كما الرسائل البريدية الإلكترونية. إن كنت تخطط لمشاركة الملفّ مع شخصٍ معيّن فقط فحينها ستحتاج كذلك إلى مفتاحه العام، وستستخدم مفتاحه العام لتشفير الملفّ ثمّ يمكنك إرساله إليه عبر أي وسيط، وسيقوم هو باستخدام مفتاحه الخاصّ لإلغاء تشفير الملفّ.

وهو سيكرر نفس العملية بالنسبة إليك؛ سيأخذ مفتاحك العام ويستخدمه لتشفير الملفّ، ثمّ

يُرسله لك عبر أي وسيط. وستستخدم أنت مفتاحك الخاصّ لإلغاء تشفير الملفّ وقراءة محتوياته.

يمكنك القيام بالعملية السابقة على أنظمة لينكس وmacOS عبر الأمر gpg. طبّق الأمر التالي أوّلًا لتصدير مفتاحك العامّ (ولا تنس استبدال بريدك الإلكتروني):

```
gpg --armor --export your@email.com > mypublickey.asc
```

ويمكنك الآن إرسال ملفّ mypublickey.asc إلى الشخص الآخر عبر أيّ وسيط ليستعمله هو في تشفير الملفّات والرسائل التي يريد إرسالها إليك.

إذا كنتَ تريد أنت أن تُرسل إليه ملفًّا مشفّرًا فعليك حينها استيراد مفتاحه العام عبر الأمر التالي (بعد أن تحصل على الملفّ منه):

```
gpg --import otherpublickey.asc
```

وبعدها، طبّق الأمر التالي لتشفير الملف المطلوب وفق المفتاح العام لذاك الشخص (لا تنس استبدال البريد الإلكتروني هذه المرّة ببريده الإلكتروني هو):

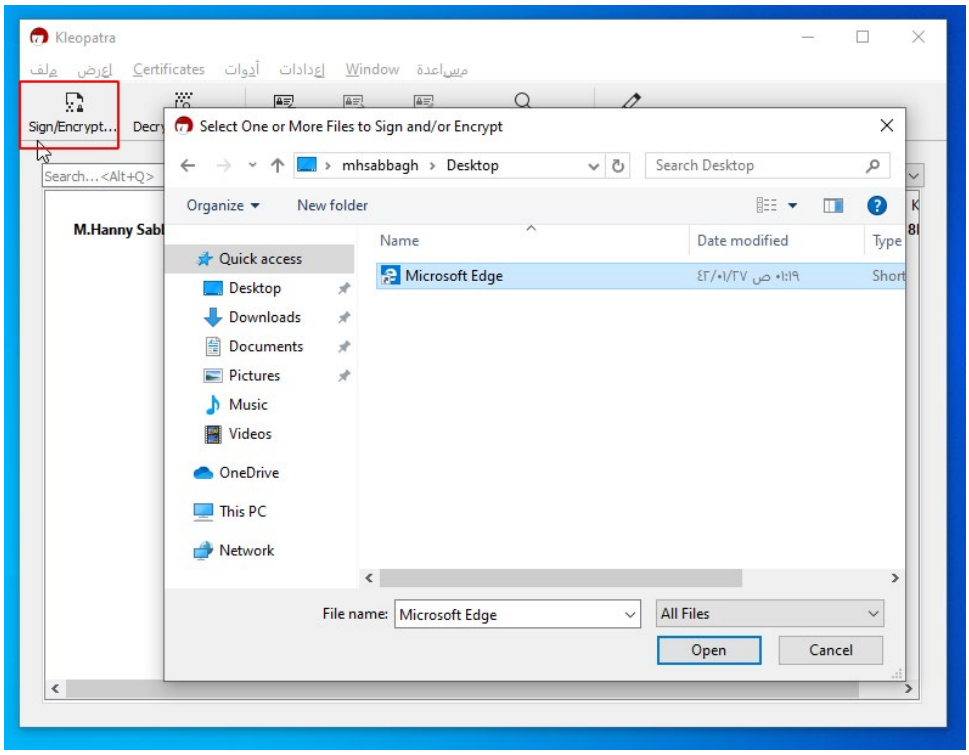
```
gpg --recipient otherparty@email.com --encrypt requested_filename.txt
```

وهكذا صار الملفّ مشفّرًا ويُمكنك إرساله إليه (ستجده باسم requested_filename.txt.gpg في نفس المسار). ويمكنه هو إلغاء تشفير الملفّات عبر الأمر التالي ثمّ كتابة كلمة المرور الخاصّة بالمفتاح الخاصّ:

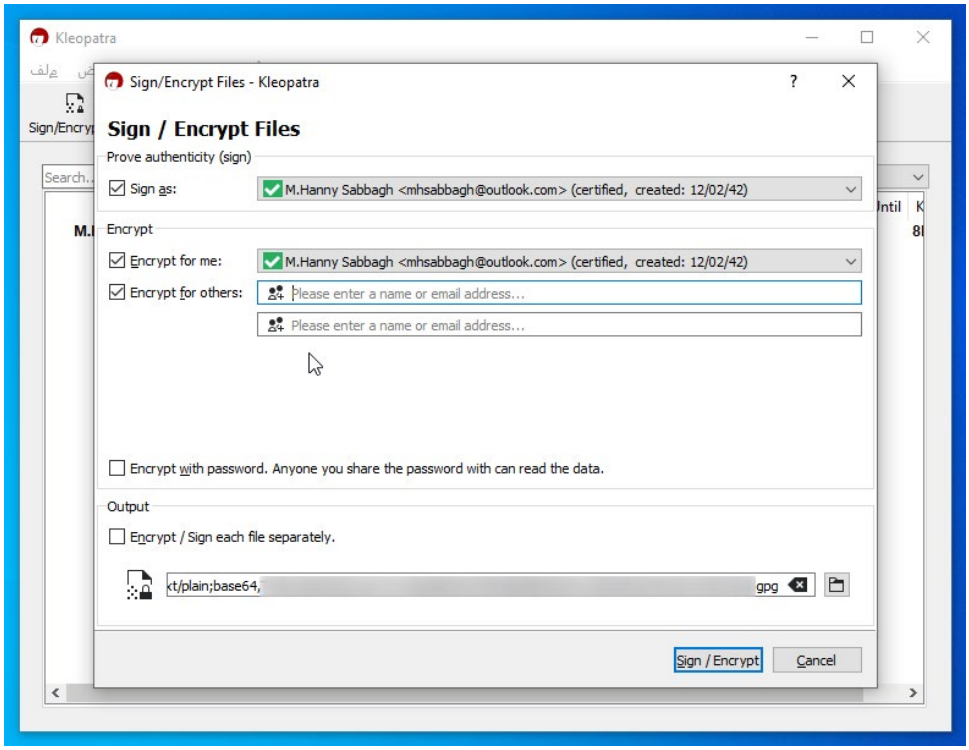
```
gpg --decrypt requested_filename.txt.gpg > unencrypted.txt
```

وستجد أنّ الملفّ قد فُكَّ تشفيره في نفس المسار وصار قابلًا للقراءة (لا تنس استبدال لاحقة الملفّات باللاحقة المناسبة مثل mp4. أو png. بناءً على نوع المحتوى، استخدمنا txt. كمجرّد مثال).

يمكنك استخدام برنامج Gpg4Win السابق على أنظمة ويندوز للقيام بنفس العملية. فقط استورد المفتاح العام للشخص المُراد التعامل معه ثمّ اضغط على "Sign/Encrypt" وحدد الملفّ المطلوب تشفيره:



ثمّ اختر اسم الشخص الذي تريد تشفير الملفّ وفق مفتاحه العام. يمكنك كذلك توقيع الملفّ رقميًا أو حمايته بكلمة مرور إضافية أن أردت ذلك:



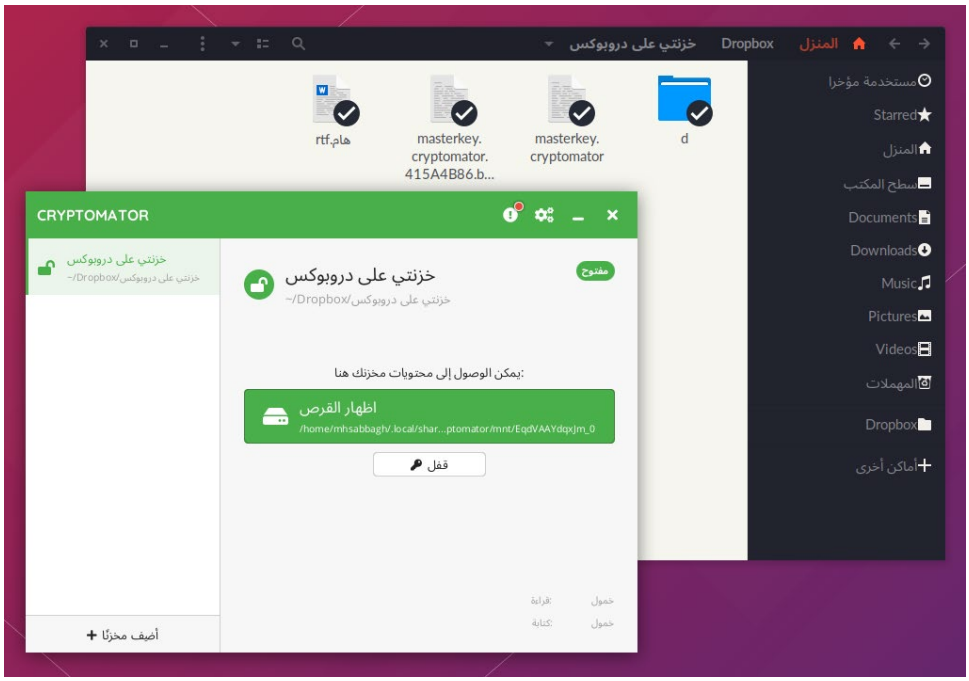
بعدها يمكنك إرسال الملفّ ومشاركته كيفما تشاء.

8.4. تشفير خدمات التخزين السحابية

إنّك غالبًا ما تستخدم خدمات المزامنة السحابية مثل Google Drive وDropbox وغيرها، لكن هل تعلم أنّه يمكنك كذلك تشفير كلّ ملفّاتك عليها؟ في النهاية هي مجرّد ملفّات، ويمكنك تطبيق نفس العملية السابقة عليها جميعها وبالتالي حمايتها من الآخرين حتّى لو وصلوا إليها بطريقةٍ ما.

إننا نستحسن استخدام برنامج Cryptomator لهذه العملية. وهو برنامجٌ مجاني ومفتوح المصدر، ويدعم تشفير كامل الملفّات وحمايتها بكلمات المرور. إننا ندعم استخدام هذا البرنامج لأنّه قد تُحقِّقَ منه ومن أمانه عبر باحثين أمنيين مستقلين (Independent 3rd-party Security Audit) ويستخدم تشفير AES بمفاتيح بطول 256 بت بصورة افتراضية، وبالتالي هو آمن للاستخدام، هذا فوق كونه مجانيًا ومفتوح المصدر ويعمل على كلّ أنظمة تشغيل الحواسيب والهواتف الشهيرة (ويندوز وماك ولينكس وأندرويد وiOS)، كما أنّه يدعم معظم - إن لم يكن كلّ - خدمات التخزين السحابية.

يقوم البرنامج بإنشاء "خزنة آمنة (Vault)" داخل مساحتك على خدمة المزامنة السحابية، وهذه الخزنة مشفّرة ومحمية بكلمة مرور (بما في ذلك اسمها!)، وكلّ ما عليك فعله هو تثبيت البرنامج ثمّ وضع ملفّاتك التي تريد حمايتها داخل تلك الخزنة، ببساطة.



8.5. ختام الفصل

التشفير تقنية قوية جدًا لحماية البيانات والملفّات والرسائل، ومن المنصوح جدًا استخدامها في تبادل البيانات الحساسة بين مختلف الأطراف. لكن لا تنسى أنّه حتّى أقوى التقنيات مثل

التشفير قد تكون قابلةً للكسر إمّا بسبب كلمات المرور الضعيفة أو بسبب البرمجيات المُستعملة في التشفير، وليس بالضرورة أن تكون خوارزمية أو تقنية التشفير نفسها بها خلل أو ثغرة أمنية.

والتشفير واحدٌ من التقنيات التي تنتهي فاعليتها تمامًا عند وجود هكذا ثغرات في البرمجيات التي تولّده أو تستعمله، ولهذا إن كنت تستخدم التشفير في مكانٍ ما على جهازك فحينها عليك التأكّد من أنّ كل برمجياتك وأدواتك محدثّة إلى آخر إصدار، وأنّها لا تحوي أي ثغراتٍ أو مشاكل أمنية معروفة (يمكنك التحقق من ذلك من مواقع أخبار الأمان الرقمي، سنشير إليها في نهاية الكتاب)، وإلّا فأنت تخاطر بكامل ملفّاتك وبياناتك ورسائلك جملةً واحدة.

9. كلمات المرور

كلمات المرور من أهمّ وسائل حماية بياناتك الحسّاسة على مختلف مواقع الويب. سيشرح هذا الفصل كل ما يتعلّق بكلمات المرور وطرق تقويتها وإدارتها.

9. 1. معايير كلمات المرور القوية

عندما تقوم باستعمال كلمة مرور معيّنة مثل "test123" على موقع إنترنت معيّن، فما تقوم به هذه المواقع هو أنّها تأخذها وتحفظها مع بقية بياناتك (اسم المستخدم وعنوان البريد الإلكتروني ...إلخ) داخل قاعدة البيانات الخاصّة بها. مواقع الإنترنت الجيّدة - ومعظمها إن لم يكن كلّها - لا تقوم بتخزين كلمات المرور بصورة صرفة (Plain Text)، بل تقوم بتشفيرها أوّلًا وفق خوارزمية معيّنة ثمّ تحفظ النصّ المشفّر، شيء مثل:

```
ecd71870d1963316a97e3ac3408c98ad8cf0f3c1bc703527c30265534f75ae
```

داخل قاعدة البيانات، أمّا كلمة المرور نفسها فلا تُحفظ أبدًا داخل قاعدة البيانات.

يُستعمل هذا الأسلوب لأنّه في حال حصل اختراقٌ من طرف المخترقين لمواقع الإنترنت هذه فحينها لا نريد أن يتمكّن المخترقون من فتح حسابات المستخدمين والوصول إليها ومعرفة كلمات مرورهم. فمن الشائع كذلك أنّ المستخدمين يستخدمون نفس كلمة المرور على أكثر من موقع ويب (وهذا أمرٌ شائع للأسف، لكنّه خاطئٌ بشدّة). وبالتالي تُقلل الأضرار عند حصول هذا النوع من الاختراقات، فهم لن يروا سوى النص المشفّر ولا يمكنهم عمل شيء به.

هناك ما يعرف باسم هجمات القوّة الغاشمة (Bruteforce Attack)، وهي هجمات مؤتمتة لتخمين كلمات المرور الخاصّة بك، حيث يبرمج المخترقون برامج وظيفتها تخمين كلمة مرور

حساباتك وتجريبها مئات وآلاف وملايين المرّات إلى أن يصلوا إلى النتيجة الصحيحة. وتعمل هذه البرامج عبر تجريب كلّ احتمالات كلمات المرور المكوّنة من 4 أحرف وأرقام مثلًا، ثمّ 5، ثمّ 6 وهكذا إلى أن يصلوا إلى كلمة المرور الصحيحة. ولهذا فإنّ استخدام كلمة مرورٍ طويلة ومعقّدة يزيد من حمايتها بصورة كبيرة.

تتضمن مواقع الويب المبنية بصورة جيّدة أنظمة مؤتمتة كذلك للحماية ضدّ هذا النوع من الهجمات، لكن ليس كلّها بالطبع.

كلّما زاد طول وتعقيد كلمة المرور، كلّما كان تخمينها عن طريق هذا النوع من الهجمات أصعب ويستغرق وقتًا أطول، وبصورة عامّة فإنّ أي كلمة مرور أطول من 8 أحرف تصبح صعبة جدًا خاصةً إن كانت مليئة بالرموز والأرقام (مثل !@#$%^&* وغيرها).

المشكلة الآن هي أنّ الكثير من المستخدمين يستخدمون كلمات مرورٍ بسيطة من السهل معرفتها أو تخمينها، أو يستخدمها مستخدمون آخرون كذلك بكثرة. وهذه مشكلة لأنّ:

- كلمات المرور القصيرة وغير المعقّدة من السهل كسرها عبر هجمات القوّة الغاشمة، حيث تستغرق وقتًا قصيرًا لتخمينها من طرف البرمجيات.
- غالبًا ما يقوم المستخدمون الآخرون كذلك باستخدام نفس كلمات المرور القصيرة لحساباتهم، فكلمة مرور مثل "123456" مثلًا ليست محصورة بشخص معيّن هو الوحيد الذي يستخدمها بل غالبًا يتشارك الملايين من الناس - للأسف - باستخدامها. الآن ماذا فعل المخترقون؟ بدلًا من الجلوس وعمل هجمة قوّة وحشية من الصفر في كلّ مرّة، أنشؤوا قواعد بياناتٍ خاصّة بهم لكلمات المرور وما يقابلها من النصوص المشفّرة التي جرّبوها بالفعل. فصاروا الآن غير محتاجين لإعادة العملية بعد أن نجحوا في كسر كلمة "123456"، بل يكفيهم النظر فيما بين أيديهم بالفعل. تُعرف هذه الهجمات باسم هجمات القاموس (Dictionary Attacks).

من أجل هذا عليك استخدام كلمات مرور قوية ومعقّدة لحساباتك المختلفة، وهذه بعض النصائح لذلك:

- اجعل كلمة المرور أطول من 8 حروف على الأقل.
- استخدم الأرقام والرموز داخلها.
- لا تكرر النصوص الفرعية داخلها؛ أي لا تستعمل شيئًا مثل "GGGG1111" فهذه كلمة مرور من الأسهل كسرها.
- لا تستعمل نفس كلمة المرور على امتداد أكثر من موقع ويب.

- لا تستعمل نمطًا معيّنًا في كل كلمات مرورك؛ بعض الناس يستعمل نمطًا كأن يكتب اسم موقع الويب الحالي ويتبعه بالرموز والحروف مثل "Twitter!123" و"Facebook\!123". هذا سيّء لأنّه بمجرّد كسر كلمة مرورك في موقعٍ واحد فسيتمكن المخترقون من التخمين أنّك تستعمل نفس النمط على مواقع الويب الأخرى، فيقومون فقط بتجريب تغيير اسم موقع الإنترنت لعلّه يعمل معهم.

الحلّ الأنسب لكلمات المرور في الواقع هو ألّا تكتبها وألّا تحتاج لتذكّرها ولا معرفتها بنفسك؛ هناك إضافات لمتصفّحات الويب وبرامج خاصّة تقوم بإنشاء كلمات مرورٍ عشوائية قوية مثل Passwordgenerator.net، حيث تطلب منها إنشاء كلمة مرور لك وتقوم هي بذلك، فتنسخ النص وتلصقه على موقع الويب عند إنشاء حسابك الجديد أو تغيير كلمة المرور.

الآن كيف ستتذكر كلمة المرور المعقّدة هذه وتدخلها كلّ مرّة؟ لن تفعل ذلك، بل ستستخدم برنامجًا لإدارة كلمات المرور، وهو ما سنشرحه في القسم التالي.

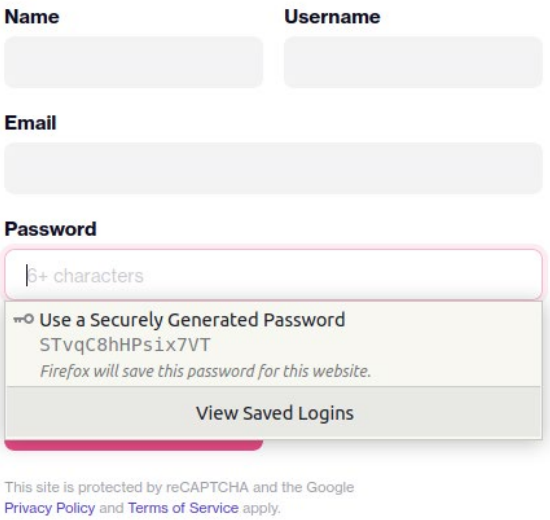
9. 2. استخدام برامج إدارة كلمات المرور

برامج إدارة المرور هي برامج خاصّة بتنظيم كلمات المرور سواءً كانت كبرامج مستقلة أو إضافات لمتصفّحات الويب الشهيرة، بل بعض المتصفّحات تتضمن برامج إدارة كلمات المرور داخلها.

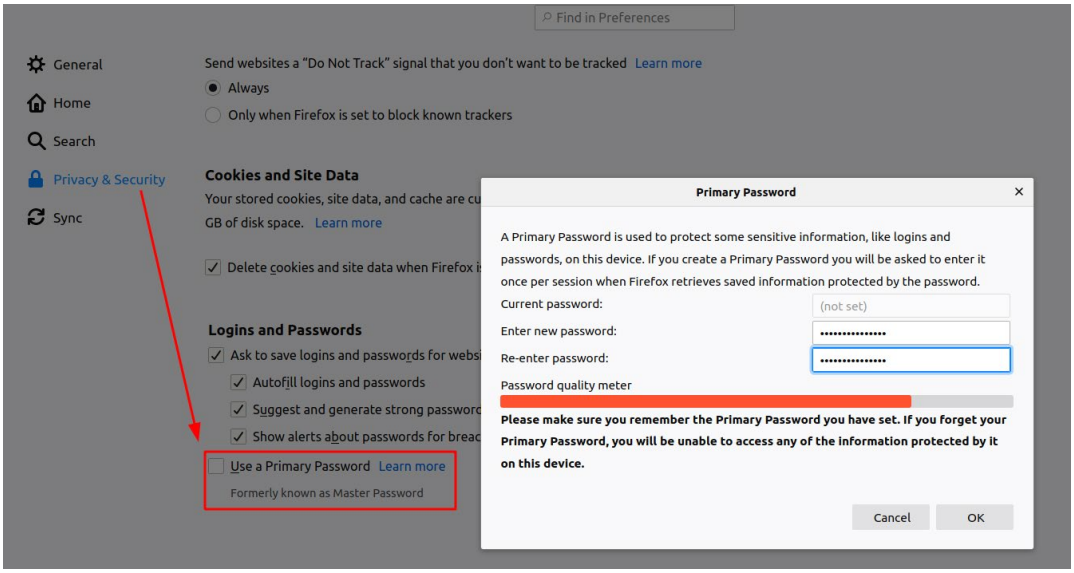
تقوم هذه البرامج بـ:

1. إنشاء كلمات المرور العشوائية القوية لك عندما تحتاج إليها.
2. حفظ كلّ كلمات المرور الخاصّة بك بصورة آمنة.
3. إنشاء ما يُعرف بـ"كلمة المرور الرئيسية" (Master Password) وهي كلمة مرور عليك حفظها وتذكّرها، وبمجرّد إدخالها في البرنامج تفتح لك خزنة كلمات المرور ويصبح بإمكانك رؤيتها وتعديلها، أمّا دون كلمة المرور الرئيسية فلا يمكن لأحدٍ الوصول لكلمات مرورك السابقة. هكذا تحتاج إلى تذكّر كلمة مرور واحدة فقط بدلًا عن جميعها.
4. إدخال كلمات المرور المحفوظة في قاعدة البيانات تلقائيًا في صفحات الويب التي تطلبها عند زيارتك إيّاها داخل المتصفّح.
5. مزامنة كلمات المرور بين مختلف أجهزتك من حواسيب وهواتف محمولة على امتداد مختلف أنظمة التشغيل التي تستعملها.

يتضمّن متصفّح فيرفكس بعض المزايا الأساسية لإدارة كلمات المرور. فهو مثلًا سيعرض عليك إنشاء كلمة مرور عشوائية قوية عند تسجيلك في مختلف مواقع الويب لأوّل مرّة تلقائيًا:



كما يدعم فيرفكس استخدام كلمة مرور رئيسية من إعداداته:



تصبح كلمات مرورك وإعداداتك متوفّرة على مختلف الأجهزة التي تستعملها عبر خدمة Firefox Sync الموجودة داخل المتصفّح.

هناك الكثير من برامج إدارة كلمات المرور المستقلة، ولكننا ننصح بالمفتوح المصدر منها فقط:

- Bitwarden: برنامج إدارة كلمات مرور يعمل على مختلف أنظمة التشغيل والهواتف المحمولة ويدعم المزامنة، كما يمتلك إضافاتٍ لمتصفّحيّ فيرفكس وكروم. يوفّر كامل شِفرتَه البرمجية على شكلٍ مفتوح المصدر.

- LessPass: إضافة لمتصفّحيّ فيرفكس وكروم، بالإضافة إلى تطبيق أندرويد وتطبيق من سطر الأوامر (CLI). تدعم المزايا الأساسية لإدارة كلمات المرور ويستخدمها الكثيرون.
- هناك الكثير غيرها لكنّ هذه أشهرها وأفضلها.

إننا ننصح بعدم تخزين كلمات المرور داخل المتصفّح وعدم الاعتماد على المتصفّح لإدارة كلمات المرور، بل استخدام أحد برامج إدارة كلمات المرور الشهيرة ثمّ تثبيت الإضافة الخاصّة به على متصفّح الويب ثمّ استعمالهما معًا. وهذا لأنّ متصفّحات الويب تفتقد الكثير من المميزات الأساسية المتعلّقة بإدارة وتأمين كلمات المرور، فيكون استخدام برامج مخصصة لذلك خيارًا أنسب.

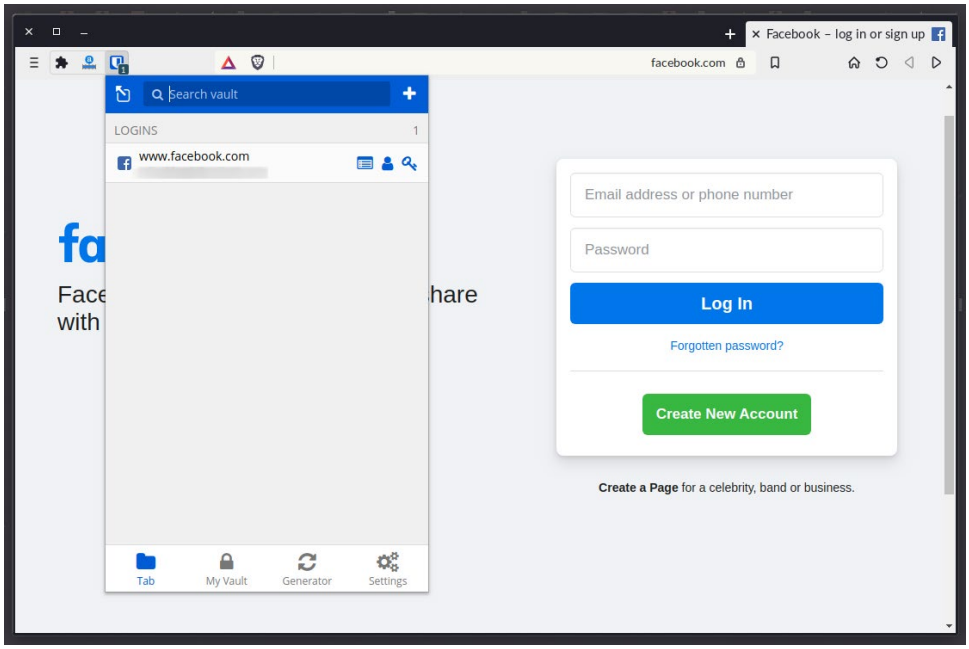
إذًا دعنا نلخّص الآن طريقة تعاملنا مع بيانات تسجيل الدخول للمواقع المختلفة (اسم المستخدم وكلمة المرور):

- ستذهب إلى إعدادات متصفّحك وتلغي السماح بحفظ وتذكّر كلمات المرور داخل المتصفّح.
- ستثبّت برنامج إدارة كلمات مرور مثل Bitwarden وغيره على جهازك، وتستورد بياناتك من متصفّحك الحالي إليه ثم تحذف كامل بياناتك من متصفّحك. لن تتبقى أيّ بيانات تسجيل دخول محفوظة على متصفّحك بل ستُنقل كلّها إلى برنامج إدارة كلمات المرور.
- ستثبّت إضافة المتصفّح الخاصّة ببرنامج إدارة كلمات المرور ذاك على متصفّحك (Integration).
- ستقوم بإدخال كلمة مرور رئيسية (Master Password) في كلّ مرّة تفتح فيها المتصفّح، وهذا لإلغاء قفل حسابك وبياناتك.
- في كلّ مرّة تريد تسجيل الدخول إلى أحد مواقع الإنترنت (فيس بوك مثلًا) ستقوم بالضغط على أيقونة الإضافة واختيار اسم المستخدم وكلمة المرور الخاصّين بك، ثم تسجّل الدخول.
- عندما تريد التسجيل في مواقع جديدة فستستعمل ميّزة إنشاء كلمات المرور العشوائية الموجودة ضمن تلك الإضافة التابعة لبرنامج إدارة كلمات المرور بدلًا من أن تفكّر بها بنفسك.
- عليك كذلك تغيير كلمات مرورك القديمة إلى كلمات مرور عشوائية جديدة حتّى أنت لا تعرفها، ثمّ حفظها داخل برنامج إدارة كلمات المرور. (يستثنى من ذلك بريدك الإلكتروني الرئيسي، عليك دومًا أن تعرف ما هي كلمة مرور بريدك الإلكتروني وهذا لتتمكن من استرجاع بقية حساباتك المربوطة به في حال حصلت مشكلة).

أنا الآن مثلًا لا أعرف ما هي كلمة المرور الخاصّة بي على فيس بوك أو تويتر، لكن هذه ليست مشكلة لأنّها مخزّنة داخل برنامج إدارة كلمات المرور وأنا أحفظ كلمة المرور الرئيسية لذاك البرنامج،

وبالتالي يمكنني جلب كلمة المرور التي أريدها في أيّ وقت. حتّى لو حذفت متصفّحي أو انتقلت إلى نظام تشغيلٍ آخر فكلّ ما عليّ فعله هو تثبيت إضافة متصفّح برنامج إدارة كلمات المرور، وبعدها ستصبح كامل بيانات تسجيل الدخول الخاصّة بي لكلّ المواقع جاهزة للاستخدام.

انظر مثلًا إلى برنامج Bitwarden (مفتوح المصدر)، بمجرّد تثبيتي لإضافته على متصفّح الويب الخاصّ بي وبمجرّد زيارة أحد مواقع الويب التي أمتلك حسابًا عليها فسيعرض عليّ إمكانية تسجيل الدخول بحسابي ذاك بنقرة زرّ واحدة (يمكن كذلك نسخ اسم المستخدم وكلمة المرور وعرضهما بصورة منفصلة):



يمكنك كذلك تثبيت برامج إدارة كلمات المرور تلك على الهواتف المحمولة (أندرويد وiOS) لاستعمالها، حيث ستنسخ كلمة المرور من البرنامج وتلصقها في مربّع الإدخال داخل المتصفّح في كلّ مرّة تريد فتح أحد حساباتك عليها.

9. 3. متابعات عمليات اختراق البيانات وتغيير كلمات مرورك

تحصل الكثير من عمليات اختراق المنصّات الإلكترونية ومواقع الويب كلّ شهر، ومن الضروري أن تبقى على اطّلاعٍ لتعلم هل أنت مشمول بهذه الاختراقات أم لا، وهل سرّبت بياناتك ومعلوماتك معها أم لا.

إليك الخدمات التالية التي يمكنها أن تنبّهك عن ذلك:

- Firefox Monitor: فقط أدخل بريدك الإلكتروني وستخبرك الخدمة ما إذا كنتَ مشمولًا بأحد الاختراقات التي حصلت مسبقًا.
- Have I Been Pwned: خدمة أخرى مشابهة مفتوحة المصدر لفعل نفس الشيء.

9. 4. الاستيثاق الثنائي

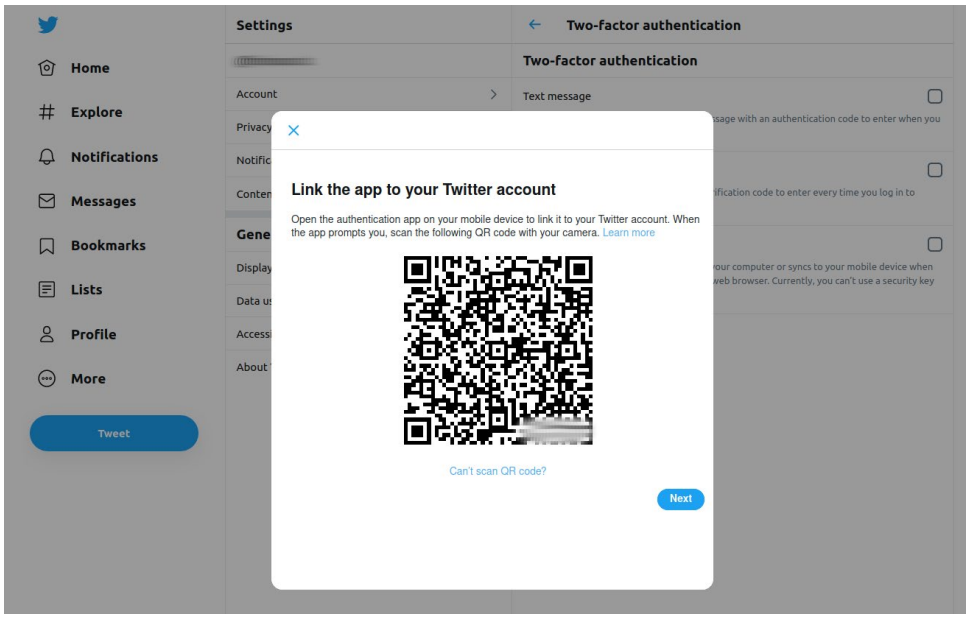
الاستيثاق الثنائي (2-Factor Authentication) هو عملية طلب المواقع الإلكترونية لوسيلة تحقق من هويّة المستخدم أكثر من مجرّد كلمة المرور؛ إمّا عبر شِفرة قصيرة تصله عبر رسالة نصّية (SMS) إلى رقم هاتفه المسجّل بالحساب، أو إلى بريده الإلكتروني أو وسيلة أخرى شبيهة. فيطلب منه موقع الويب تلك الوسيلة بعد أن يقوم بإدخال كلمة المرور الصحيحة، ولا يكتفي بكلمة المرور لفتح الحساب.

الاستيثاق الثنائي مفيد خصوصًا في التعاملات البنكية والمالية، وهذا لأنّك لا تريد لأحدهم تدمير حياتك فقط لأنّه امتلك كلمة المرور الخاصّة بك.

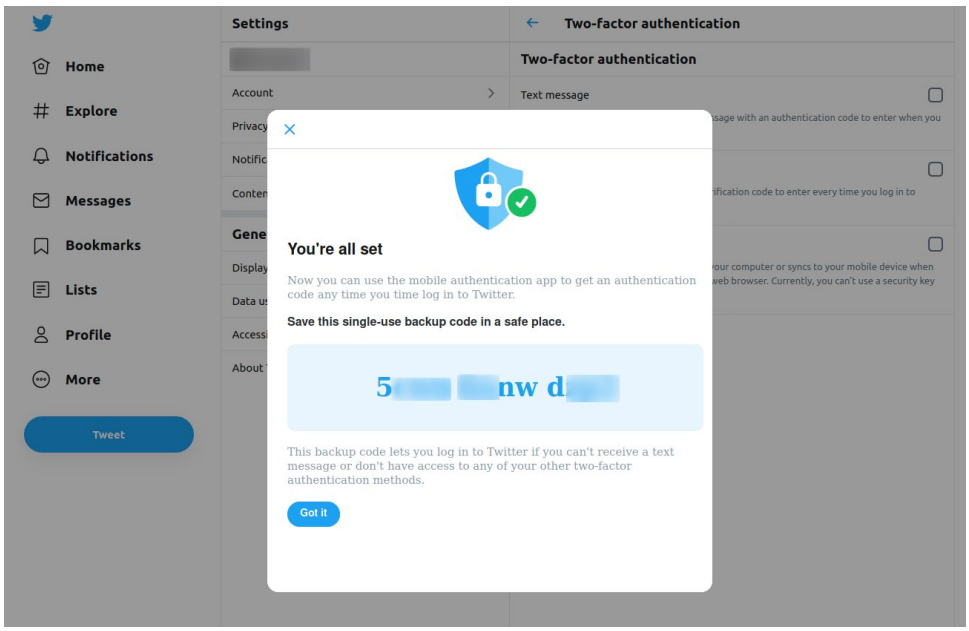
أشهر طريقة حالية للاستيثاق الثنائي هي عبر استخدام تطبيقات خاصّة بذلك على الهواتف المحمولة، حيث تقوم أوّلًا بإضافة الخدمات التي تستعملها إلى هذه التطبيقات، ثمّ عندما تريد تسجيل الدخول إليها، تقوم بإدخال رمز الأمان (Security Code) الظاهر على هذه التطبيقات والذي يتغير كلّ 30 ثانية إلى موقع الويب. هناك عدّة تطبيقات للاستيثاق الثنائي على الهواتف، أشهرها Google Authenticator ولكننا لا ننصح به بل ننصح بـFreeOTP وهذا لأنّ هذا الأخير مفتوح المصدر ومُطَوّر من طرف شرك ريدهات (Red Hat) المعروفة بتطوير البرمجيات المفتوحة المصدر للشركات.

لا تدعم كلّ مواقع الويب خاصّية الاستيثاق الثنائي، لكن تدعمها تلك الشهيرة منها مثل فيس بوك وتويتر وجوجل وكلّ التطبيقات المالية.

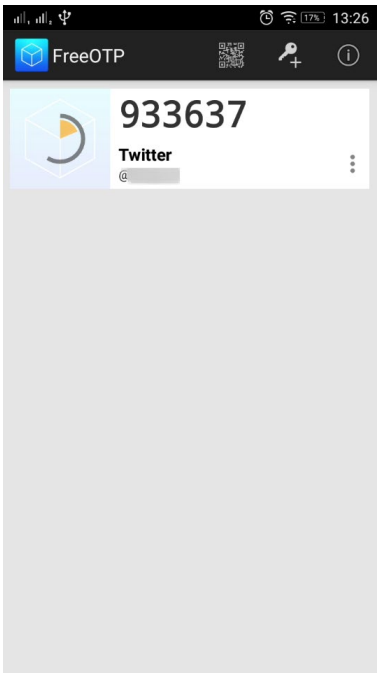
يمكنك الوصول إلى الميّزة من الإعدادات --> الأمان --> الاستيثاق الثنائي على تويتر مثلًا. سيطلب منك الموقع أن تمسح صورة الرمز عبر تطبيق الاستيثاق الخاصّ بك:



بعد أن تفعل ذلك، سيعطيك الموقع ما يُعرف برمز الاستعادة (Backup Code) ومن المهم جدًا أن تحتفظ به وألّا تنساه، لأنّه في حال سُرق منك هاتفك المحمول أو حُذف التطبيق بالخطأ فقد لا تتمكن من فتح حسابك مرةً أخرى من دونه:



ثم سيُضاف رمز الاستيثاق إلى التطبيق الخاصّ بك:



بخصوص رموز الاستعادة (Backup Codes) فإننا ننصح بطباعتها على ورقة ثمّ حذفها من الحاسوب بالكامل وعدم تخزينها في أي مكانٍ رقمي، وهذا لأنّه ستسمح باختراق حساباتك بمجرّد الوصول إليها ومن غير الآمن تخزينها رقميًا. هذا فضلًا عن أنك قد تحتاج إليها في حال السفر أو انقطاع الكهرباء.

9. 5. ختام الفصل

كلمات المرور هي الحاجز الأمني الأساسي الذي يمنع المتطفّلين من الولوج إلى حساباتك على مختلف المواقع والخدمات التي تستعملها، لذا لا تتردد بتاتًا بصرف القليل من وقتك وجهدك على تأمينها بصورة قوّية قبل أن تتابع روتينك اليومي من الاستعمال. فيكفي أن يُخترق حسابٌ واحدٌ من الحسابات الأساسية التي تستعملها لتجد نفسك في الكثير من وجع الرأس بل وعرضةً لفقد المال والملفّات والبيانات المهمّة.

10. تأمين متصفحات الويب

سيشرح هذا الفصل بعض المفاهيم الأساسية عن متصفّحات الويب وطريقة عملها، بالإضافة إلى طريقة تأمين متصفحيّ فيرفكس وكروم بصورةٍ أساسية. من المفترض أن يعمل نفس الشرح على كلّ المتصفّحات المبنية عليهما كذلك، مثل كروميوم Chromium و Ungoogled Chromium وغيرها.

تعتمد معظم الأمور المشروحة في هذا الفصل على تثبيت إضافاتٍ خارجية لزيادة مستوى الأمان والخصوصية في متصفّحات الويب، وهي على مستويات فما قد يحتاج إليه أكثر الناس مختلف عما قد يحتاج إليه المتخصص الذي يبحث عن حمايةٍ أكبر. قسّمنا الفصل بناءً على هذا الأساس كذلك.

10. 1. مفاهيم تأسيسية حول متصفحات الويب

هناك الكثير من متصفّحات الويب لأنّها تخدم أغراضًا مختلفة، وهي تستعمل كذلك محركاتٍ مختلفة (Engines)؛ فالمحرّكات هي أنوية المتصفّحات المسؤولة عن تصيير وعرض محتوى الويب بدلًا من أن يكون مجرّد شِفرات صرفة لا يمكن الاستفادة منها.

يستعمل متصفّح فيرفكس محرّك "Gecko" الخاصّ بفيرفكس نفسه وهناك بعض المتصفّحات الأخرى المبنية عليه، بينما يستعمل كروم محرّك "Blink" القادم من متصفّح كروميوم (تذكّر أننا شرحنا في السابق أنّ كروم مبني على كروميوم)، ولهذا السبب فإنّ طريقة عمل المتصفحين بالإضافة إلى طريقة عرضهما لمواقع الويب مختلفة. ولهذا السبب فإنّ بعض المواقع قد تعمل على الأوّل ولكن ليس الثاني والعكس (لكنّها قليلة جدًا في الوقت الراهن حيث صارت معايير تطوير

المواقع الموحّدة معروفة وشائعة). ولنفس السبب لا تعمل إضافات فيرفكس على كروم والعكس، لأنّهما يستخدمان محرّكاتٍ مختلفة.

متصفّح الويب كأيّ برنامج موجود على نظامك؛ له وصولٌ إلى كامل نظامك وملفّاتك بالإضافة إلى العتاد الموجود مثل الميكروفون والكاميرا، وبالتالي قد تمتلك مواقع الويب وصولًا إليها كذلك (أو لا) بناءً على ما يسمح متصفّح الويب لها أن تمتلك. وهذا هو نظام الأذونات (Permissions) الموجود في كلّ المتصفّحات الشهيرة.

لا تسمح المتصفّحات لمواقع الويب بسرد محتويات أيٍ من مجلّدات نظامك وملفّاتك افتراضيًا، لكن يمكنها الوصول إليها ورفع أجزاءٍ منها في حال طلبت هي ذلك ووافقت أنت على ذلك فقط عبر تنبيهٍ يُعرض لك قبل أن تتم العملية.

ولهذا فإنّ عملية تطوير متصفّحات الويب عملية معقّدة ومهمّة؛ فتطوير المحرّكات يحتاج سنواتٍ طويلة من العمل ليثمر والكثير من الموارد، كما أنّ تطوير متصفّحات ويب آمنة لمنع المواقع السيئة والخبيثة من سرقة بيانات المستخدمين دون علمهم مهمّة أصعب. لكنّ كلًا من متصفحيّ فيرفكس وكروم ممتازان في هذه الناحية.

ولهذا يمتلك المتصفّحان أنظمةٍ مبنية داخلهما بالفعل لاكتشاف المواقع الخبيثة التي تحاول تجاوز المتصفّح للوصول إلى الملفّات أو الكاميرا والميكروفون دون علم المستخدم، ثمّ منعها وحجبها عن المستخدم تلقائيًا.

نريد أن ننتقل الآن إلى شرح بعض الأمور العامّة عن طريقة عمل المتصفّحات مع مواقع الويب:

- نظام أسماء النطاقات (Domain Name System - DNS): لقد شرحنا ماهيّة نظام الـDNS في فصل "المفاهيم الأساسية" من هذا الكتاب بالإضافة إلى طريقة تغييره على مستوى الموجّه (Router)، لكننا نريد الإشارة هنا إلى أنّ المتصفّحات قادرة على استعمال نظام DNS مختلف عن المُستَخدم حاليًا على كامل النظام، بل يمكن حتّى للإضافات الخارجية المثبّتة فعل ذلك. في فيرفكس مثلًا هناك خيار لاستخدام نظام الـDNS التابع لشركة CloudFlare، وإذا استخدمته، فستتخلص من مشكلة تسريب الـDNS (ما يعرف بـDNS Leak) لكن داخل متصفّح الويب فقط وليس التطبيقات الأخرى.
- الاتصال بوسيط أو بلا وسيط (Proxy): الوسيط أو البروكسي هو خادومٌ يتوسّط الاتصال بين متصفّحك وبين مواقع الويب التي تريد طلبها، فاستخدامه يشبه ما تفعله في الحياة

الواقعية من أن تطلب من أحدهم إحضار شيءٍ لك من مكانٍ ما لتجنب فعل ذلك بنفسك، وهو نفس المبدأ هنا. حيث يؤدّي استخدام الوسيط إلى تجنّب حظر المواقع أو معرفة المواقع التي تزورها عبر قيام متصفّحك بالاتصال بخادومٍ وسيط ليقوم الوسيط هو بجلب الصفحات له. تستخدم متصفّحات الويب إعدادات وسيط النظام افتراضيًا لكن يمكن كذلك جعلها تستخدم وسيطًا خاصًّا بها، إمّا من الإعدادات أو عبر إضافاتٍ خارجية.

- الشهادات (Certificates): عند زيارتك لأحد مواقع الويب التي تستخدم بروتوكول HTTPS فإنّ متصفّحك يتأكّد من موثوقية هذا الاتصال وأنّه ليس مزوّرًا أو معبوثًا به من طرفٍ خارجي عبر ما يُعرف بـ"الشهادة"، وهي في الواقع حزمة بيانات (اسم صاحب الموقع والمؤسسة والجهة المسؤولة عن الشهادة بالإضافة للمفتاح العام للتشفير... إلخ) يعرضها موقع الويب لمتصفّحك ثمّ يقوم المتصفّح بموازنتها مع النسخة المحفوظة لديه (القادمة منذ تثبيت المتصفّح أو تحديثه من الجهات التي تصدر شهادات الاستيثاق لمواقع الويب) للتأكّد من هوية الموقع وصحّة الاتصال. حيث يتحقق متصفّحك من المفتاح العامّ الذي تعرضه الشهادة ثمّ المفتاح العام المُستخدم لتشفير الاتصال، ثمّ يوازن بينهما مع المفتاح العام المحفوظ لديه عن الجهة التي أصدرت الشهادة للتأكّد من صحّة الاتصال، فهو بالتالي يستعمل جهة خارجية لعمل هذا التحقق.
- ملفّات تعريف الارتباط (Cookies): إذا اشتريت قطعة حلوى من بائع الحلوى في يومٍ ما ثمّ ذهبت في اليوم التالي لشراء قطعةٍ أخرى، فقد يتذكرك بائع الحلوى ويقول: "آه أنت الذي اشترى الحلوى الفلانية بالكميّة الفلانية يوم أمس" وهذا بالضبط ما تفعله مواقع الويب مع ملفّات تعريف الارتباط؛ وهي ملفّات تخزّن بعض الإعدادات والبيانات عن نشاطاتك وتفضيلاتك في مواقع الويب التي تزورها لتقوم المواقع باستخدامها لاحقًا. جاءت تسمية هذه الملفّات كذلك بـ"الكعكات" (Cookies) من هذا الاستخدام. لا تحتوي ملفّات تعريف الارتباط عادةً أيّ معلوماتٍ شخصية عنك مثل اسمك أو بريدك أو بياناتك البنكية أو ما شابه، لكنّها تحوي مُعرّفًا خاصًّا بك (ID) يُمكّن مواقع الويب نفسها من معرفتك عندما تعود إليها في المستقبل. لكن بسبب حجم ملفّات تعريف الارتباط وكثرتها فإنّه يمكن استخدامها في الكثير من الأحيان للتعرّف على هوية المستخدمين الحقيقية، والمؤسف أنّها تُشَارك كذلك بين مختلف مواقع الويب وليس فقط المواقع التي تزورها. (وهو ما يعرف بـ"3rd-party cookies sharing"، يمنع فيرفكس وSafari مشاركتها افتراضيًا، لكن كروم يسمح بذلك). يمكن قراءة المزيد عن

ملفّات تعريف الارتباط وكيف تُستخدم لتعقّب المستخدمين من الورقة البحثية الشهيرة: "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild".

- الذاكرة الخبيئة (Cache): تقوم متصفّحات الويب بتخزين بعض الصور وملفّات التنسيق والمعلومات المختلفة عن مواقع الويب التي زرتها لتجنّب تحميلها من جديدة في المستقبل لزيادة سرعة التحميل عندما تفتحها مرّة أخرى. لكن هذا بالطبع قد يكشف بعض المواقع التي كنتَ تزورها.
- مُعرّف المُستخدم (User-Agent): معرّف المستخدم هو وصفٌ لمتصفّح الويب تأخذه خواديم مواقع الويب (Web servers) عند زيارتك إيّاها، ويحتوي اسم المتصفّح وإصداره ونظام التشغيل الحالي وإصداره واسم المحرّك وإصداره.
- بصمة الإصبع (Fingerprint): يوفّر متصفّح الويب لمواقع الويب التي تزورها الكثير من المعلومات عن نفسه بالإضافة إلى نظام التشغيل الحالي؛ مثل عتاد الجهاز وإصداره وإصدار تعريفات البطاقة الرسومية (Graphics Card)، والخطوط وقائمة الإضافات المثبّتة والمنطقة الزمنية ولغة المتصفّح ولغة نظام التشغيل، بالإضافة إلى معلوماتٍ عديدة أخرى. وهذه مشكلة لأنّه يمكن معرفة هويّة المُستخدم الفريدة من بين ملايين المستخدمين عبر مجموعة المعلومات هذه، لأنّها مختلفة جدًا بين بعضها البعض لكلّ مستخدم ومن النادر أن تجد مستخدمين اثنين من بين الملايين لتتوافق بصمة الإصبع لهما بنسبة 100%. ويظنّ الكثير من الناس أنّ تعقّبهم ومعرفة هويتهم مستحيلة إن استخدموا اتصال "في بي إن" وغيّروا نظام الـ DNS الخاصّ بهم واستخدموا هوية وهمية على الإنترنت، ولكن هذا غير صحيح في الواقع والسبب هو بصمة الإصبع، حيث أنّ استخدامك لنفس المتصفّح بنفس الإعدادات وعلى نفس نظام التشغيل سيمكّن مواقع الويب - إن شاءت - من ربط هويتك الوهمية بهويتك الحقيقية (مثل أن تقوم بعمل حسابين اثنين على أحد مواقع الويب، فيمكن لمواقع الويب أن تعرف أنّك وراء الحسابين عبر هذه الطريقة مهما فعلت). والمشكلة الحقيقية هو أنّه لا توجد حماية كاملة منها فمواقع الويب بحاجة إلى بعض هذه المعلومات لمعرفة كيف تعرض الصفحة بصورة جيّدة لك، ومنع بصمة الإصبع بالكامل أو تغييرها بصورة جذرية قد يحطّم صفحات الويب ويجعلها تتوقف عن العمل. يمكنك رؤية بصمة الإصبع لمتصفّحك الحالي عبر موقع https://panopticlick.eff.org
- التاريخ والبيانات المحفوظة: تقوم متصفّحات الويب بحفظ جميع الصفحات التي تزورها افتراضيًا لتمكينك من الرجوع إليها إن أردت، كما قد تقوم بحفظ اسم المستخدم وكلمات

المرور الخاصّة بك بالإضافة إلى معلوماتك البنكية والأمور التي تبحث عنها في مربّعات البحث على المواقع المختلفة، ويمكنك ضبط إعدادات التاريخ هذه (أو تعطيلها إن أردت) من إعدادات كلّ متصفّح.

- الطلبات (Requests): عندما تزور موقع ويب معيّن وتتصفح بعض الصفحات داخله فإنّك تقوم بإجراء "طلبات" لخادوم الويب الذي يستضيف الموقع بالصفحات التي تتصفحها، بما في ذلك محتويات تلك الصفحات من صور وسكربتات جافاسكربت وملفّات مختلفة أخرى. فعند طلبك موقع facebook.com مثلًا في المتصفّح فإنّ المتصفّح يجري العديد من الطلبات في الخلفية (Background) في الواقع قد تصل إلى مئات الطلبات لمصادر مختلفة. جميع طلباتك هذه مسجّلة لدى خادوم الويب بالإضافة إلى كلّ نشاطاتك من بحث ورفع وتصفّح وحذف وغير ذلك ضمن موقع الويب نفسه (وهي بالتالي ظاهرة لأصحاب مواقع الويب، فيمكنهم معرفة أنّ محمد هاني صبّاغ قد بحث عن الشيء الفلاني في مربّع البحث الساعة كذا يوم كذا... إلخ). ومن الممكن كذلك أن يستمر الموقع في تحديث نفسه بالخلفية عبر اتصالٍ حيّ (Live Connection) لا يُغلق عند انتهاء تحميل الصفحة، بل يستمر حتّى بعد تحميلها للمرّة الأولى لتحميل المحتوى الجديد، مثلما يفعل موقع تويتر مثلًا من تحميل التغريدات الجديدة عند توفّرها، وهذا يؤدي إلى طلباتٍ مستمرة من طرف متصفّحك لتحميل هذه البيانات الجديدة.

10. 2. ضبط إعدادات المتصفّحات الافتراضية

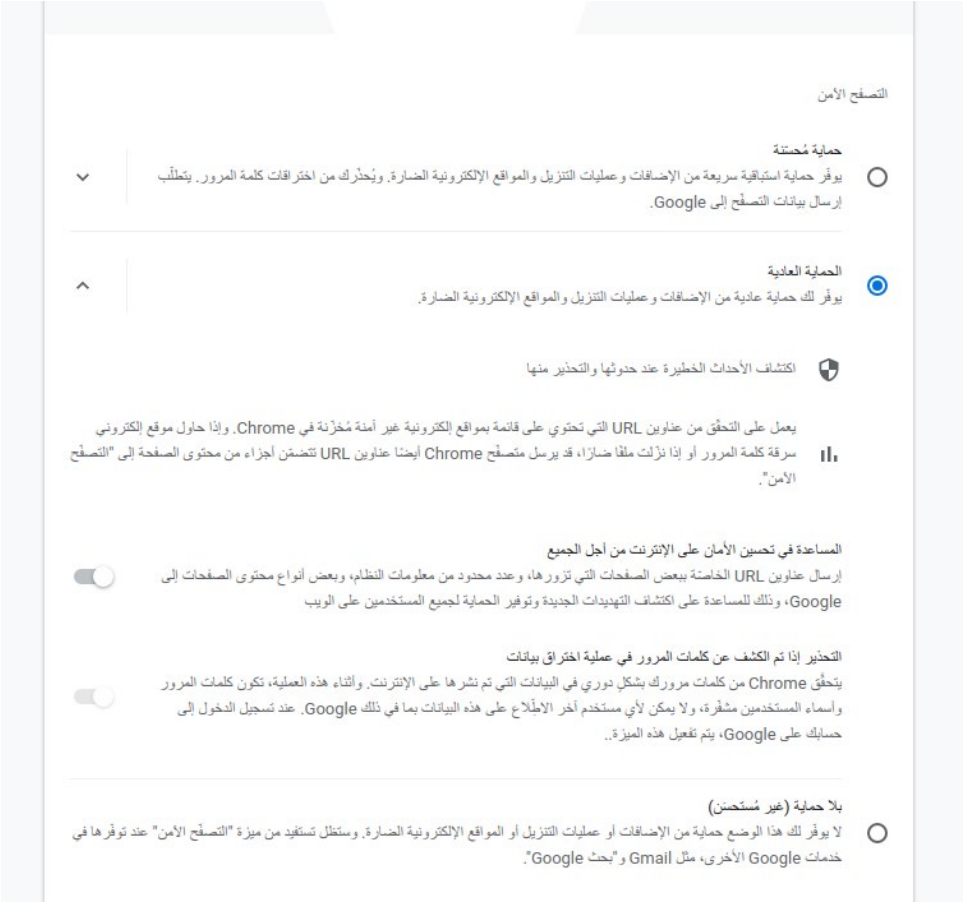
يأتي كلٌ من متصفحيّ فيرفكس وكروم بإعداداتٍ افتراضية تسمح للمتصفّح أن يُرسل بياناتٍ عنك وعن نشاطاتك على الشبكة. يمكنك تعطيلها لزيادة مستوى الخصوصية.

في فيرفكس، اذهب إلى التفضيلات (Preferences) --> الخصوصية والأمان (Privacy & Security)، وعطّل خيارات "جمع Firefox للبيانات واستخدامها (Firefox collection for data)" بالشكل التالي:

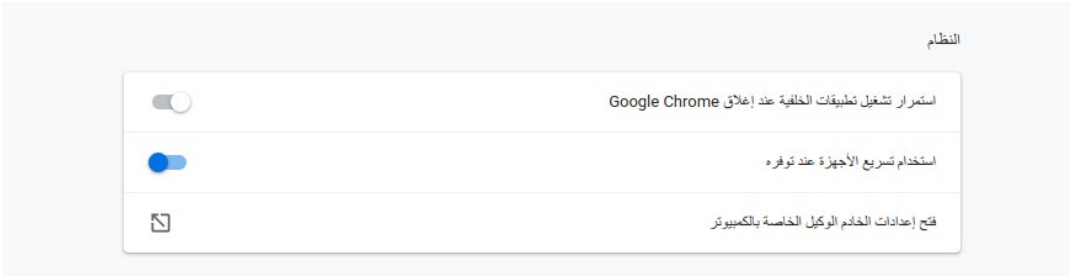
هنـاك الكثيـر مـن الإعـدادات الأخـرى المتعلّقـة بالخصوصيـة فـي فيرفكـس مـن نفـس الصفحـة. يمكنـك مراجعتهـا جميعًـا وضبطهـا لتناسـبك، مثـل حـذف كلّ التاريـخ عنـد إغـلاق المتصفّـح مثـلًا أو إبقـاؤه لمـدّة معيّنـة فقـط أو مـا شـابه ذلـك.

فـي كـروم، اذهب إلى الإعـدادات (Settings) --> خدمـات Google والمزامنـة (Google Services & Synchronization) وعطّـل خيـارات تسـجيل الدخـول إلـى حسـاب جوجـل ومشـاركة البيانـات والبقية بالشـكل التالي:

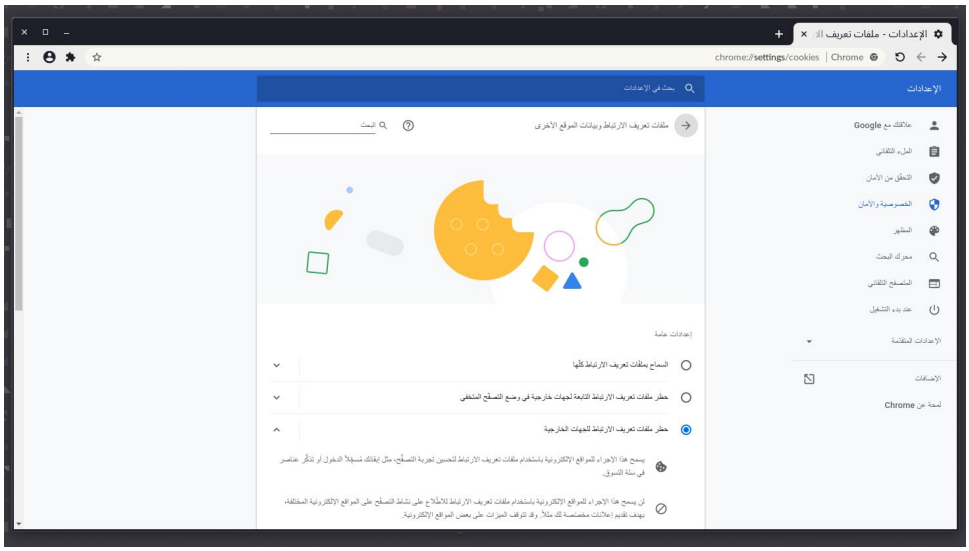
يمكنـك كذلـك الذهـاب إلـى أمـن المعلومـات (Information Security) وتعطيـل خيـار مشـاركة مواقـع الويـب التـي تزورهـا والبيانـات الأخـرى كالتالـي:



تحتاج كذلك إلى منع كروم من الاستمرار في العمل في الخلفية، وهذا لتجنّب جمع أي شيءٍ متعلّق بك أو الوصول إلى العتاد مثلًا:



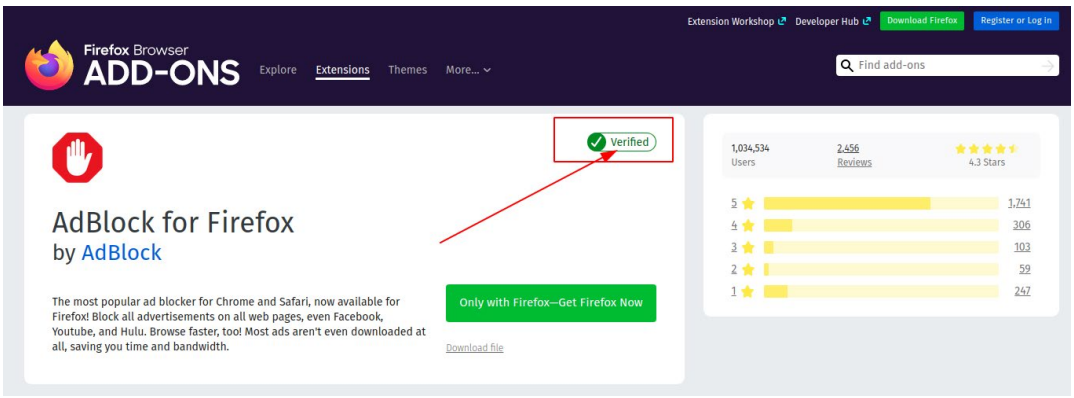
أخيرًا عليك تعطيل مشاركة ملفّات تعريف الارتباط (Cookies) مع جهات الطرف الثالث (3rd-Party) لمنع مواقع الويب من معرفة نشاطك على المواقع الأخرى، بل تسمح لها بمعرفة نشاطك السابق على الموقع ذاته فقط (فلا يمكن لفيس بوك معرفة تفضيلاتك على جوجل، بل يمكن لجوجل معرفة نشاطك على مواقع جوجل وحدها فقط):



10. 3. إضافات لتوفير الخصوصية لمتصفحات الويب

تدعم معظم متصفّحات الويب الحديث ما يُعرف بـ"الإضافات"، وهي برمجيات صغيرة تُضاف إلى المتصفّح لتمكينه من أداء مهام لم يكن قادرًا على فعلها من قبل. عليك استخدام إضافات موثوقة فقط ومن مصادر معروفة، فالإضافات كالبرامج يُمكن أن تستعمل إمّا لزيادة أمانك وخصوصيتك أو لاختراقك.

حاول ألّا تثبّت أيّ إضافة متصفّح بعددٍ أقل من 10 آلاف مستخدم ولها تقييم وسمعة جيدة على متجر الإضافات. يوجد على متجر إضافات فيرفكس علامة "Verified" وهي تعني أنّ مهندسي موزيلا قد اطّلعوا على الشِفرة المصدرية للإضافة ولم يجدوا بها أي مشكلة، وهذه الإضافات هي أأمن إضافات يمكنك تثبيتها:



للأسف لا يوجد شيء مماثل لذلك على متجر إضافات كروم، ولذلك إن كنت تستعمل أيّ متصفّح ويب مبني على كروميوم فأنت متروكٌ لتواجه المعضلة وحدك وفق حدسك (عدد التحميلات، عدد المراجعات، اسم الشركة المطوّرة وسمعتها ...إلخ).

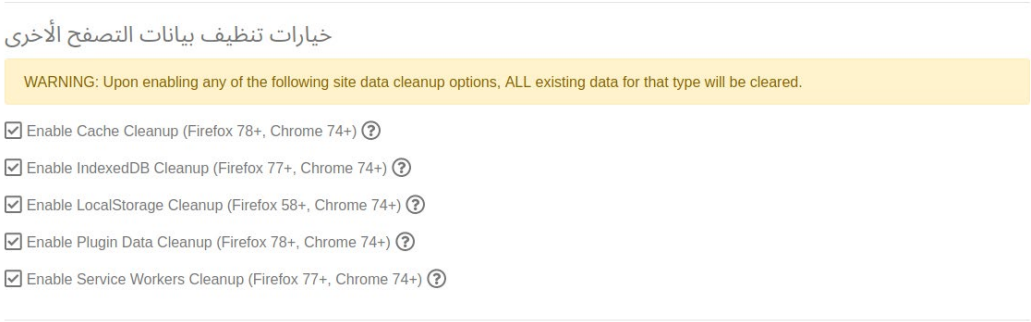
لاحظ أنّ هذه الإضافات قد لا تحميك من تعقّب بصمة الإصبع (Fingerprinting) وقد يتوجّب عليك البحث عن غيرها لتأمين نفسك. يمكنك التحقق دومًا من كونك مؤمنًا ضد هذا النوع من الهجمات أم لا عبر الموقع التالي: https://panopticlick.eff.org. ومن تجربتنا وجدنا أنّه لا يوجد أفضل من الإعدادات الافتراضية لمتصفّح Brave للحماية ضدها فهو لا يحتاج أيّ إضافات بل يحميك منها مباشرةً بعد التثبيت.

10. 3. 1. إضافات أساسية لا غنى عنها

- uBlock Origin: الإضافة الأشهر والأقل استهلاكًا للموارد لحجب الإعلانات والنوافذ المنبثقة والكثير من السكربتات السيئة على الويب. ستحجب كل الإعلانات بمجرّد تثبيتها على متصفّحك. (فيرفكس، كروم)
- Privacy Badger: إضافة من EFF (مؤسسة المكافحة الرقمية، مؤسسة موثوقة) لحجب سكربتات التعقب التي تنتهك خصوصية المستخدم وتجمع معلوماتٍ حوله. ستعمل بمجرّد تثبيتها كذلك وسترى أيقونةً في شريط أدوات المتصفّح تخبرك ما السكربتات التي سُمِح بها وما التي مُنعت. (فيرفكس، كروم)
- HTTPS Everywhere: من EFF كذلك، تقوم بتحويل المستخدم تلقائيًا إلى إصدار بروتوكول HTTPS بدلًا من HTTP في حال توفّره (حيث لا تقوم بعض المواقع بذلك تلقائيًا). (فيرفكس، كروم)
- Cookies AutoDelete: تقوم هذه الإضافة بحذف ملفّات تعريف الارتباط (Cookies) تلقائيًا عند إغلاق التبويب (Tab) المُرتبط بها بالإضافة إلى ملفّات التخزين المحلّية (Local Storage) والذاكرة الخبيئة (Cache) وغيرها من الإعدادات المحفوظة، وبالتالي تمنع مواقع الويب من تعقّبك بصورةٍ مستمرة ومعرفة نشاطاتك على مواقع الويب الأخرى المفتوحة حاليًا (وستحتاج بالطبع تطوير عادةٍ في إغلاق التبويبات المفتوحة بمجرّد الانتهاء منها). استخدامها سيعني كذلك أنّه سُيسَجّل خروجك تلقائيًا من المواقع التي سجّلت الدخول إليها (فيس بوك، جوجل ...إلخ) تلقائيًا بمجرّد إغلاق كافّة التبويبات المرتبطة بها، ولكن هذا ثمنٌ رخيص مقابلة حماية خصوصيتك على الشبكة بهذا الشكل الهائل.

لتفعيل الإضافة بصورةٍ صحيحة فإنّه يتوجّب عليك تفعيل خيار "تمكين التنظيف التلقائي (Enable Auto Clean up)" من إعدادات الإضافة، ثمّ ضبط "ثانية تأخير قبل التنظيف التلقائي (Seconds before clean up)" إلى 1. (أي أنه ستُحذف جميع ملفّات الارتباط وغيرها بعد ثانية

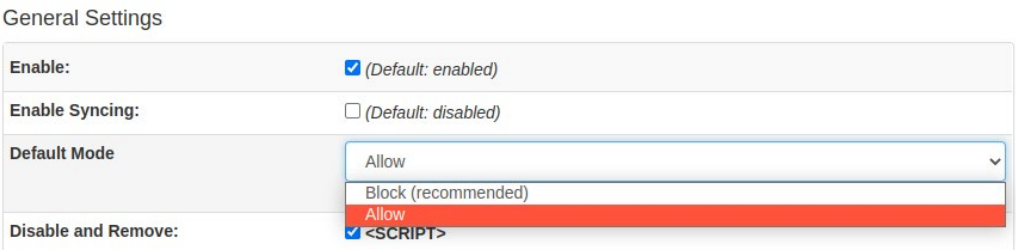
واحدة من إغلاق التبويبات). ستحتاج كذلك إلى تعطيل الإشعارات والسجل (Notifications & Log) بالكامل لمنع عرض الإشعارات المزعجة بصورة مستمرة. وأخيرًا، ستحتاج تفعيل الخيارات التالية:



الإضافة متوفّرة لمتصفحيّ فيرفكس وكروم.

10. 3. 2. إضافات لخصوصية أكبر

- Remove Google Redirection: إن الروابط التي تراها في نتائج بحث جوجل تأتي مضمّنةً بروابط تعقّب من شركة جوجل، ولهذا إن حاولت نسخ الرابط من نتائج البحث ولصقها في مكانٍ آخر فستجد رابطًا طويلًا من جوجل ليس هو في الواقع الرابط الحقيقي الذي رأيته في نتائج البحث. تقوم هذه الإضافة بحلّ المشكلة ببساطة عبر وضع الرابط الحقيقي لنتائج البحث بدلًا من رابط التعقّب لجوجل (فيرفكس، كروم)
- ScriptSafe: إضافة خاصّة بمتصفّح كروم لإدارة كلّ ما يتعلّق بالأمان والخصوصية فيه. تأتي الإضافة بوضع المنع افتراضيًا ولهذا ستحتاج تغييره إلى وضع السماح (Allow by default) لتجنّب تحطيم مواقع الويب:



يمكنك الآن تصفّح خيارات الإضافة وتفعيل أو تعطيل ما تريده. لاحظ أنّ الإضافة ستعرض لك كلّ أسماء النطاقات التي تحاول تتبعك أو جمع معلوماتٍ عنك في شريط أدوات كروم (من أيقونة الإضافة). توفّر الإضافة حمايةً ضدّ تقنيات تتبع بصمة الإصبع (Fingerprinting) بالإضافة إلى حماية من تتبع معرّف المُستخدم (حيث يمكنك تخصيصه إلى واحدٍ مشترك بين معظم المستخدمين)

وحماية من تسرّب عناوين الآي بي عبر WebRTC والحماية من معرفة الصفحة المُحِيلة إلى الصفحة الحالية (Referrer Spoof) وغير ذلك الكثير. (كروم).

- NoScript: بما أنّ الواجهة الأمامية لمواقع الويب تستعمل الكثير من شِفرات جافاسكربت لتصيير صفحات الويب وتسهيل عرضها وعمل العديد من الأشياء (وهي الشفرات القادرة على تتبع المستخدمين وجمع البيانات عنهم كذلك) فإنّ حلّ هذه الإضافة للمشكلة كان ببساطة عبر منع كل شِفرات جافاسكربت افتراضيًا إلّا تلك التي يسمح لها المستخدم. لكن لاحظ أنّ هذا المنهج سيؤدّي إلى تعطّل معظم مواقع الويب ولهذا قد تحتاج الكثير من التمرّس في إعدادات هذه الإضافة لتتمكن من استخدامها بصورة مريحة، إلّا أنّها فعليًا الإضافة الوحيدة التي توفّر الحماية القصوى الممكنة من مواقع الويب فهي تمنع كلّ السكربتات من العمل إلا ما تسمح له أنت (فيرفكس، كروم).

10. 4. خدمات مزامنة بيانات المتصفح

تمتلك معظم متصفّحات الويب مثل فيرفكس وكروم خدمات مزامنة (Sync Services) مبنية داخلها لمزامنة بيانات تصفّحك وكلمات مرورك ومعظم نشاطك الذي تجريه عبر متصفّح الويب (التاريخ، بيانات النماذج، العلامات... إلخ). وهي خدمات مدمجة داخل المتصفّحات نفسها دون الحاجة لتثبيت أيّ إضافاتٍ أخرى.

إننا لا ننصح باستخدام أيّ خدمة مزامنة، فهذا يعني تخزين كامل تاريخ تصفّحك ومعلوماتك الحساسة وبيانات اسم المستخدم وكلمة المرور الخاصّة بك في مكانٍ واحد أنت لا تأتمنه حقًا؛ فوضع كامل بياناتك مع جوجل سيكون مشكلة بسبب انتهاكات جوجل المعروفة للخصوصية. المزامنة مع فيرفكس أأمن وأكثر ثقةً لكنّها عرضة أيضًا لعددٍ من الهجمات المحلّية على الجهاز فجميع البيانات مخزّنة في مكانٍ واحد وبالتالي يمكن ربط بيانات اسم المستخدم وكلمة المرور مع بيانات تصفّحك الأخرى.

لا تضع كلّ البيض في سلّة واحدة.

لقد نصحنا في السابق بعدم تخزين كلمات المرور داخل المتصفّح بل استخدام برنامج إدارة كلمات مرور (Password Manager) لفعل ذلك. وهذا هو ما نستحسنه هنا أيضًا؛ إزالة الحاجة لخدمات المزامنة والاكتفاء ببرامج إدارة كلمات المرور مثل Bitwarden لإجراء عمليات تسجيل الدخول والخروج. يمكنك استخدام إضافات خارجية لمزامنة بعض أنواع المحتوى مثل الملاحظات أو العلامات، لكن لا تعتمد على خدمات المزامنة داخل المتصفّح.

هكذا تبقى جميع ملفّاتك مخزّنة محليًا على جهازك دون أن تغادره (أو في مكانٍ آخر)، بينما تبقى بياناتك الحساسة منفصلة عن بيانات ومعلومات تصفّحك الأخرى ومؤمنة بصورة منفصلة. ولن تحتاج التعامل لا مع موزيلا ولا مع جوجل.

استعمالك لأكثر من خدمة لا علاقة بينها لتخزين أنواع مختلفة من المحتوى هو خيارٌ أفضل من استخدام خدمات المزامنة الموحّدة داخل المتصفّحات.

10. 5. خاتمة الفصل

كانت هذه هي المعلومات الأساسية التي تحتاج معرفتها وضبطها عند استخدامك متصفّحات الويب الشهيرة. قد يكون الموضوع صعبًا ويتطلب الكثير من العمل للوهلة الأولى عند قراءة هذه الأشياء إلّا أنّها لن تستغرق نصف ساعة أو ساعة بالكثير، وما ستحصل عليه في المقابل من حفاظ خصوصيتك ومنع المتطفلين ومواقع الويب من مراقبة نشاطاتك رائعٌ جدًا مقابل ما صرفته من وقتٍ وجهد.

عمليات التعقّب وانتهاكات الخصوصية على الإنترنت كثيرة وشائع وتتطور باستمرار ولا تتوقف، ولذلك ستحتاج متابعة قراءة آخر التطوّرات في المجال لضمان حمايتك بصورة مستمرة.

11. الحماية من مواقع الإنترنت

إنّ مواقع الإنترنت هي الجبهة الأولى لانتهاكات الخصوصية والأمان الرقمي الخاصّين بالمستخدم، فهي ما يتعامل المستخدم معه يوميًا ويقضي معظم وقته عليه. ولذلك من المهم أن يكون المستخدم واعيًا بأفعاله عليها وما يمكن لها أن تكشف عن هويته.

سيشرح هذا الفصل أساسيات الوعي المتعلّقة بالتعامل مع مواقع الويب والتسجيل فيها.

11. 1. الانتباه إلى نتائج البحث

إنّ نتائج البحث التي تراها في أيّ محرّك - مثل جوجل وغيره - تُوصل إلى مواقع ويب مختلفة. لكن ما لا يعرفه الكثير من الناس هو أنّ مواقع الويب هذه قادرةٌ على معرفة الكلمة المفتاحية التي كتبها المستخدم في محرّك البحث ليصل إلى الموقع، وبالتالي يمكن لها معرفة أنّ عنوان الآي بي الفلاني قد وصل إلى الموقع عن طريق تلك الكلمة المفتاحية (مثل أن تكتب "إدارة الوقت" في جوجل مثلًا ثمّ تفتح أحد المواقع، فسيعرف ذلك الموقع أنّك كتبت "إدارة الوقت" في جوجل لتصل إليه).

وليس في هذا ضررٌ كبير على الخصوصية من الوهلة الأولى، فالمواقع الكبيرة والضخمة لا تحاول تتبع هويّات المستخدمين بهذا الشكل. لكن إن كنت تسأل عن الناحية العملية التقنية فمن الممكن لهذه المواقع أن تربط الكلمات المفتاحية التي تبحث عنها في جوجل بحساباتك المسجّلة عليها؛ فهم يمتلكون الآن عنوان الآي بي الحقيقي الخاصّ بك وهويتك الحقيقية بعد تسجيلك لديهم، وهم لديهم وصولٌ إلى الكلمات المفتاحية التي استعملتها لتصل إلى مواقعهم من محرّكات البحث، وبالتالي يمكنهم ربط هذه المعلومات ببعضها البعض إن أرادوا لمعرفة المزيد من المعلومات عنك.

وحلّ هذه المشكلة عبر منع ما يسمّى بـ"Referral Page" (الصفحة المُحِيلة) وهيّ ميّزة في

متصفّحات الويب تسمح للصفحة التالية أن تعرف ما هي الصفحة السابقة التي أحالت إليها. ويمكنك منعها عبر البحث عن إضافات خارجية لمتصفّحات الويب في متجر الإضافات الخاصّ بمتصفّحك، وقد تحتاج بعض الوقت لضبطها بصورة صحيحة فبعض المواقع قد تتوقف عن العمل إن منعتها بشكلٍ كامل.

لاحظ كذلك أنّ بعض الجهات قد تستخدم ظهورها في نتائج البحث كنوعٍ من الهندسة الاجتماعية لتضليل المستخدمين (المزيد عن الهندسة الاجتماعية في فصولٍ لاحقة)، مثلًا توكد البنوك على ضرورة التأكد من عنوان موقع البنك عند الدخول عليه لكي لا يكون هنالك شكل مشابه لموقع البنك نفسه يريد خداعك بسرقة معلوماتك وبيانات حساباتك البنيكة.

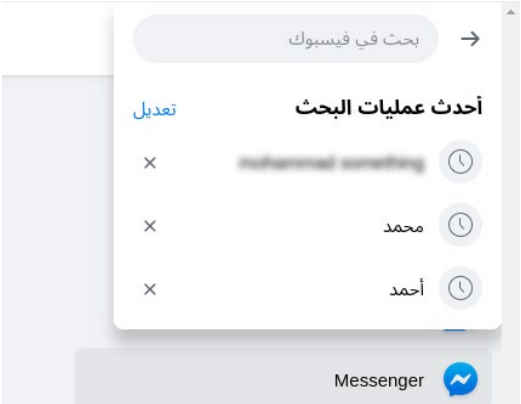
نقرك على واحدٍ من هذه الروابط - ولو لمرّة واحدة - قد يؤدّي إلى تسجيل عنوان الآي بي الخاصّ بك لديهم إلى الأبد وبالتالي ربط الكتب التي تقرأها وتحمّلها من موقعهم بهويتك الحقيقية التي هم قادرون على اكتشافها بفضل قدرات التجسس والوصول إلى بيانات الشركات الأجنبية لديهم (فهم لديهم عنوان الآي بي الحقيقي الخاصّ بحسابك على فيس بوك بالفعل مثلًا، وبالتالي يمكنهم ربطه - نظريًا - بالكتب التي تحمّلها من عندهم).

عليك كمستخدم تجنّب النقر على نتائج بحث من مواقع مشبوهة أو تحمل أسماءً غريبة، أو تمتلك أسماء نطاقات غير مفهومة.

11. 2. عمليات البحث والسجلات في مواقع الإنترنت

تدعم معظم مواقع التواصل الاجتماعي مثل فيس بوك وتويتر ميّزة البحث، حيث يمكنك البحث عن منشورات أو صور أو فيديوهات لأشخاصٍ معينين.

لكن لا ينتبه بعض الناس إلى أنّ عمليات بحثهم هذه مسجّلة في مواقع التواصل، وبالتالي إن نجح أحدهم في الوصول إلى الحساب بطريقةٍ ما أو حتّى رآك وأنت تتصفحه من بعيد فسيعرف أنّك كنت مهتمًا بأشخاصٍ معينين أو تبحث عنهم بسبب ذلك:



يمكنك الضغط على زرّ تعديل لتنتقل إلى صفحة سجلّ البحث الخاصّة بك، ويمكنك بعدها إزالة كامل السجلّ عبر الضغط على "مسح عمليات البحث" كالتالي:

في فيس بوك بالتحديد الوضع أكثر صعوبة فعمليات البحث - حتّى بعد حذفها - لا تُزال من قاعدة بيانات الموقع الفعلية تمامًا، بل ستلاحظ مثلًا أنّك إن بحثت عن شخصٍ معين وتصفّحت حسابه عدّة مرّات، فستجد اسمه دومًا في أوّل قائمة "تسجيلات الإعجاب" أو قائمة "المشاركات" على المنشورات المختلفة التي تراها على فيس بوك. وهذه ميّزة تنتهك الخصوصية بصورة صارخة ولا يبدو أنّ أحدًا قد انتبه إليها من قبل.

يسجّل تويتر كذلك عمليات البحث ويمكنك إزالتها من زرّ "مسح الكل" (Clear all):

جوجل قصّة أخرى فكل نشاطاتك على خدماتها مسجّلة (عمليات البحث على محرّك بحث

جوجل، البحث في يوتيوب، كل مواقعك الجغرافية في خرائط جوجل ...إلخ) لكن لحسن الحظّ يمكنك تعطيلها من الرابط: https://myactivity.google.com

فقط افتح الرابط ثمّ اذهب إلى "إدارة عناصر التحكم في نشاطك" (Control your Activity Controls)، ثمّ عطّل جميع الخيارات الموجودة في الصفحة مثل:

- النشاط على الويب وفي التطبيقات.
- سجل المواقع الجغرافية.
- سجل YouTube.
- تخصيص الإعلانات.
- وغيرها.

لاحظ أنّ نشاطك السابق ما يزال محفوظًا، لكن يمكنك حذفه عبر "إدارة النشاط" (Manage Activity) ثم طلب حذف كلّ السجلّ من هناك، وعليك تكرار العملية لكل نوعٍ من أنواع السجلات الموجودة. لاحظ كذلك أنّ جوجل لن تعطّل عمليات تخزين السجلات بصورة دائمة بل لفترة مؤقتة فقط، ولذلك عليك التحقق من كون السجلّات معطّلة كلّ فترة.

قد تكون السجلّات مفعّلة كذلك في بعض الخدمات الأخرى التي تستخدمها، ويمكنك التحقق من كونها موجودةً أم لا من إعدادات ذاك التطبيق ثم حذفها إن أردت ذلك. الموضوع بسيط كما ترى ولا يحتاج سوى بضع دقائق لحذف وتعطيل كلّ شيء، وهو فقط جولة في الإعدادات لا أكثر.

11. 3. رسائل البريد الإلكتروني الكاشفة للهوية

يمتلك المستخدم العادي عشرات وربّما مئات الحسابات على مختلف مواقع الويب وقد يستعمل في بعضها أسماءً وهمية لا تمثّله حقيقةً، لكن قد يربطها بالبريد الحقيقي الخاصّ به وهذه

مشكلة لأنّ هذه المواقع ستراسلك غالبًا في الكثير من الأحيان ذاكرةً الاسم الذي تستعمله عليها (رسائل مثل العروض الترويجية أو استعادة كلمات المرور أو الإعلانات وما شابه ذلك) بالإضافة إلى معلوماتٍ أخرى حساسة متعلّقة بالمواقع تلك.

وبما أنّ عنوان البريد الإلكتروني ثابت للمستخدمين فهذا يؤدّي إلى تراكم آلاف الرسائل البريدية داخل صندوق البريد على مدار السنين. وبالتالي أي وصول إلى بريدك الإلكتروني سيكشف تلك البيانات كذلك، لأنّ المُخترِق (أو الشركة المزوّدة للخدمة البريدية في حال طلب قضائي مثلًا) سيتمكنون من الوصول إلى جميع الرسائل وبالتالي معرفة كلّ الحسابات المرتبطة به مباشرةً.

حلّ تلك المشكلة هو ببساطة عبر إيقاف خيارات المُراسلة البريدية من تلك الخدمات نفسها، حيث تمنعها من إرسال رسائل بريدية لك إلّا في حال الضرورة القصوى (مثل استعادة كلمات المرور مثلًا) ثمّ تحذف تلك الرسائل مباشرةً من صندوق بريدك بمجرّد أن تنتهي منها.

يمكنك الوصول إلى إعدادات المُراسلة البريدية للخدمات هذه من إعداداتها. كلّ شيء موجود في الإعدادات :)

11. 4. التسجيل في المواقع وإعطاء معلوماتك لها

ضع في بالك أنّك تسلّم المعلومات التالية للمواقع الإلكترونية والخدمات عندما تسجّل فيها:

- عنوان الآي بي الحالي الخاصّ بك.
- اسم جهازك الحالي (Hostname).
- معرّف المستخدم (User-agent) الخاصّ بمتصفّحك.
- بصمة الإصبع (Fingerprint) الخاصّة بمتصفّحك.
- جميع البيانات المطلوبة منك في نموذج التسجيل.

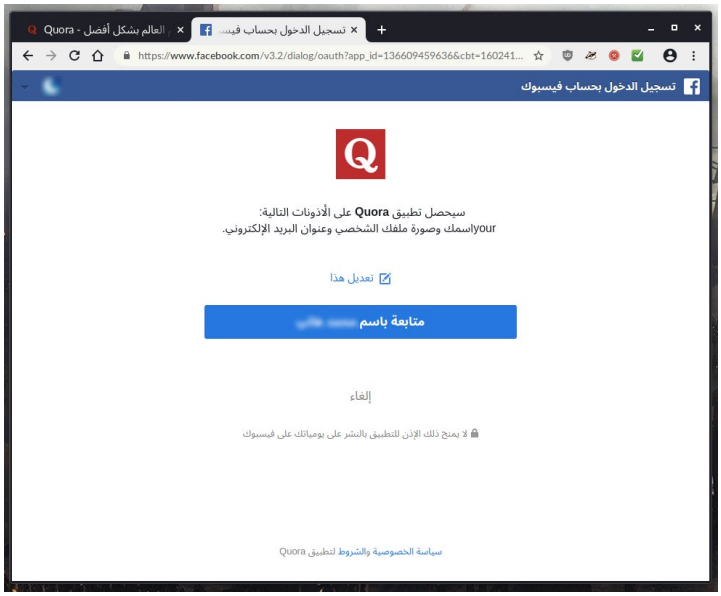
يمكن لمواقع الويب أن تأخذ هذه المعلومات مجددًا - إن أرادت - عند كلّ طلب جديد (Request) تُرسله إليها، كما يمكنها الاحتفاظ بأكثر من نسخة منها إن شاءت لموزانتها وبالتالي تعقّب المستخدمين بصورة أكبر ومعرفة من فتح أكثر من حسابٍ عليها.

ومن أجل هذا ننصح بعدم استخدام نفس المتصفّح ونظام التشغيل لفتح الحسابات الوهمية؛ بل عملها عبر متصفّحات آمنة بالإضافة إلى استخدام إضافات تغيير معرّف المستخدم وتعطيل خاصّيات بصمة الإصبع، بحيث تضمن أنّ هذه المعلومات مختلفة تمامًا عن معلومات حسابك الحقيقي وبالتالي لا يمكن المطابقة بينهما.

11. 5. تطبيقات الطرف الثالث (3rd-Party Apps)

تتيح معظم مواقع التواصل الاجتماعي وعددٌ كبير من الخدمات الأخرى ما يسمّى بـ"دعم تطبيقات الطرف الثالث" (3rd-Party Apps). سمّيت هذه التطبيقات بتطبيقات "الطرف الثالث" لأنّ الطرف الأوّل هو المستخدم، والطرف الثاني هو الخدمة نفسها بينما هذه التطبيقات هي من جهة خارجية أخرى، ولهذا سمّيت بالطرف الثالث.

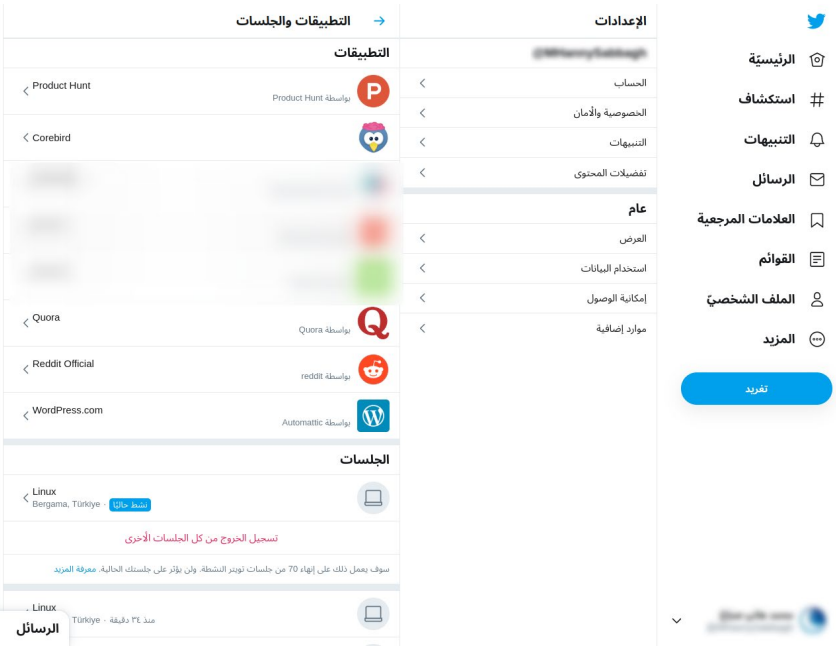
هذه التطبيقات هي مثل الاندماجات (Integrations) للخدمة التي تستعملها، مثل تسجيل الدخول إلى أحد المواقع الإلكترونية (موقع كورا مثلًا Quora.com) عن طريق حسابك على فيس بوك أو تويتر، وستلاحظ أنّ الموقع سيطلب منك إضافته كتطبيق إلى حسابك وبالتالي إعطائه بعض الصلاحيات عليه:



من المهم جدًا أن تفهم ما الصلاحيات التي تطلبها هذه التطبيقات منك قبل الموافقة عليها، وذلك لأنّ بعضها قد يكون خبيثًا ويتسبب في سرقة حسابك بالكامل أو بعض المعلومات منه. وفي الواقع هذه واحدة من أكثر الطرق شيوعًا لاختراق الحسابات والخدمات الإلكترونية؛ ألّا تُخترق الخدمة نفسها بل تطبيقات الطرف الثالث التي تعمل على تلك الخدمات مما يؤدّي بالتالي إلى اختراق حسابات المستخدمين الذين كانوا يستعملونها.

لأنّه بما أنّ تلك التطبيقات لديها وصولٌ إلى حسابات آلاف المستخدمين - وفق الأذونات والصلاحيات التي سمحوا بها لها - فبالتالي من الممكن اختراق تلك التطبيقات بدلًا من محاولة اختراق حسابات المستخدمين أنفسهم أو المنصّة الإلكترونية نفسها، وهذا أسهل للمخترقين، فهو هجومٌ واحد يشنّونه على التطبيق بدلًا من عشرات الآلاف من الهجمات على المستخدمين.

يمكنك رؤية التطبيقات الحالية التي فعّلتَها على حسابك بالإضافة إلى الصلاحيات التي تمتلكها من إعدادات الحساب، ثمّ ابحث عن تطبيقات الطرف الثالث، كما في تويتر مثلًا:



إن انتهيت من أحد هذه التطبيقات ولم تعد تخطط لاستعماله في المستقبل فأزله مباشرةً من حسابك.

لا تقبل بتاتًا بإضافة أيّ تطبيقٍ لا تعرفه أو لا تثق به أو لا تعرف مصدره، وتجنّب الموافقة على التطبيقات الشخصية (التي يطوّرها أفراد وليست باسم شركات) فهي أدعى لأن تكون خبيثة وأسهل للاختراق.

تُخترق شهريًا بيانات ملايين المُستخدمين حول العالم بسبب تطبيقات الطرف الثالث [1].

11. 6. خاتمة الفصل

إن تعاملك مع المواقع الإلكترونية المختلفة بوعيٍ وتفكير منفتح على الأمان والخصوصية هو أكبر عاملٍ قد يحميك وبياناتك من الاختراق أو المشكلات مستقبلًا. بضع دقائق من الاكتراث لهذه الأشياء قد تحميك من خسارة الكثير من الوقت والمال والجهد مستقبلًا. فالحذر الحذر عزيزي القارئ!

12. ما يلزم معرفته عند الشراء والدفع عبر الإنترنت

سيشرح هذا الفصل بعض الأمور والإجراءات المهمّة عند إجراء عمليات الشراء والدفع عبر الإنترنت، وهذا لتأمين بياناتك البنكية الحسّاسة وتجنّب تسريبها أو اختراقها وبالتالي حصول مصائب مالية لك.

إن اتباع هذه النصائح والمعلومات أساسي لتجنّب المشاكل المالية التي قد تلحق بك والتي قد تضطرك إلى الاتصال بالشرطة أو مراجعة البنك في حال فقدانها أو اختراقها، ودرهم وقاية خيرٌ من قنطار علاج!

12. 1. موثوقية المواقع التي تشتري منها

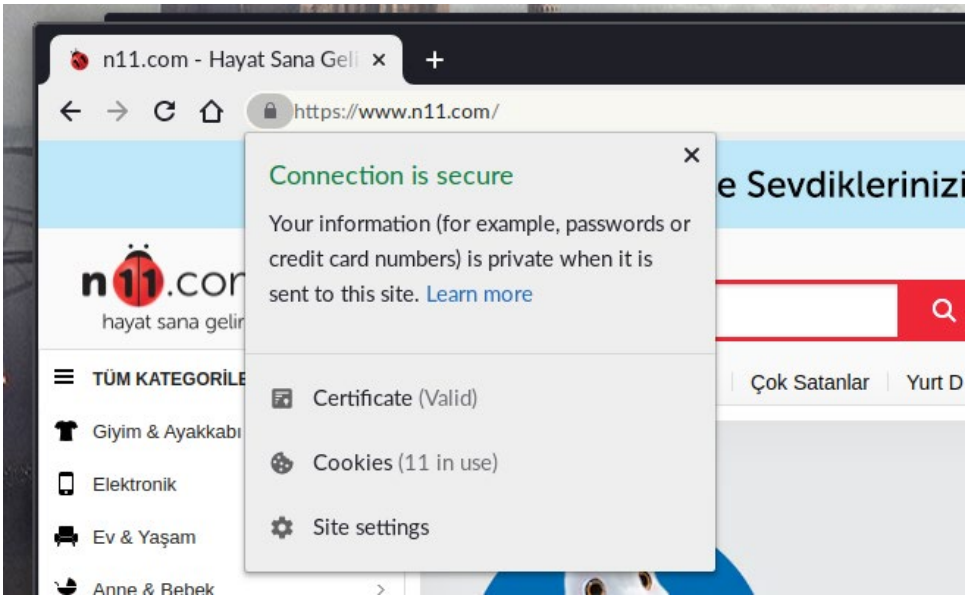
عليك تجنّب المواقع غير المعروفة والصغيرة بشكل عام وعدم إجراء معاملات مالية معها، فأنت لا تدري مدى موثوقيّتها وهل ستستعمل بيانات البطاقة الائتمانية الخاصّة بك بصورة آمنة أم لا.

هناك إضافة اسمها Alexa Rank (فيرفكس، كروم) تظهر لك ترتيب موقع الويب الحالي داخل المتصفّح في شريط الأدوات من بين كامل مواقع الويب الأخرى وفق ترتيب أليكسا الشهير؛ وهو ترتيبٌ لمواقع الإنترنت كلّها بناءً على مدى شهرتها. وبالتالي يمكنك تقدير عدد زوّار ومستخدمي الموقع بناءً على الرقم الظاهر لك (مثلً فيس بوك وجوجل يحتلان المركزين الأوّل والثاني وهذا لأنّهما يخدمان مليارات المستخدمين يوميًا... وكلّما ازداد الرقم كلّما قلّ عدد الزيارات التقديري له).

ننصح بصورة عامّة ألّا تتعامل مع أيّ موقع تجاري على الإنترنت يكون ترتيبه أقلّ من 500 ألف، فهذا يعني أنّه يستقبل أقل من 500 زيارة يوميًا.

انظر كذلك في الموقع الذي تريد التعامل معه؛ هل يوفّر سياسة خصوصية وشروط مالية واضحة بين صفحاته أم لا؟ هل معروفٌ من يقف وراءه أم لا وهل هناك متابعون آخرون له على مواقع التواصل الاجتماعي أو مراجعات جيّدة على Google Reviews أم لا؟ ستساعدك كلّ هذه المعلومات في تقرير ما إذا كان من الآمن التعامل معه.

الشيء الثاني لتنظر فيه هو استخدام الموقع لاتصال HTTPS؛ وهو ما يعني أنّ الاتصال بينك وبين موقع الويب مشفّر ولا يمكن للمتطفلين أن يتجسسوا على البيانات المتبادلة بينكما، وبالتالي تحمي بياناتك البنكية من السرقة أو الاختراق. يمكنك معرفة ذلك عبر النظر في شريط العنوان وستجد أنّ الإشارة الخضراء مع كلمة «HTTPS» موجودة:



لا تدخل بطاقاتك الائتمانية بتاتًا في أيّ موقع ويب لا يستعمل تشفير HTTPS، فهذا التشفير أساسي للمعاملات البنكية وأيّ موقع لا يستعمله يعني أنّه موقع رديء الجودة وغير قادر على تأمين بياناتك البنكية بصورة جيّدة.

12. 2. تأمين بطاقاتك الائتمانية

سيطلب منك أيّ موقع تجاري على الإنترنت البيانات التالية لإجراء المعاملات المالية:

- رقم البطاقة الائتمانية المكوّن من 16 رقم.
- اسم الشخص حامل البطاقة.
- تاريخ نفاذ صلاحية البطاقة.
- شِفرة الأمان (CVC) الموجودة على البطاقة من الخلف.

قد تعرض عليك مواقع الإنترنت المختلفة حفظ معلوماتك الائتمانية لديها لتجنّب إدخالها في كلّ مرّة تريد الشراء فيها، لكننا ننصح بشدّة برفض ذلك وعدم حفظها وهذا لأنّك لا تدري كيف يقوم موقع الويب بتأمين هذه المعلومات، وبالتالي يُمكن أن يُخترق الموقع في المستقبل وتُسرّب معلوماتك الائتمانية كلّها وتُستخدم من طرف الآخرين وتحصل مشاكل طويلة وعريضة. بدلًا عن ذلك لن يأخذ إدخال معلومات البطاقة منك يدويًا سوى 30 ثانية كحد أقصى لكنك ستكسب راحة بالك إلى الأبد.

إن كنت تريد التعامل مع موقع ويب لا تعرف مدى مصداقيته بالكامل فيمكنك إنشاء ما يُعرف بالبطاقة الائتمانية الوهمية (Virtual Credit Card) من تطبيق البنك الخاصّ بك على الهاتف المحمول؛ وهي بطاقة تابعة لبطاقتك الائتمانية الرئيسية لكن بحدّ مالي (Limit) تحدده أنت ويكون أقل من الحدّ المالي الكامل للبطاقة الأصلية. تمتلك هذه البطاقة رقمها الخاصّ المختلف عن البطاقة الأصلية.

وهكذا حتّى لو كان الموقع خبيثًا ويريد بالفعل سرقة معلوماتك فإنّه لن يقدر على الوصول إلى البطاقة الحقيقية وسيسحب فقط من البطاقة الوهمية التي تُدخل معلوماتها، كما يكون حدّها المالي أصغر بكثير - وفق ما ترى أنت - من البطاقة الأصلية وهكذا تحمي بطاقتك الأصلية وأموالك من السرقة.

إليك هذه النصائح الإضافية لتأمين معلوماتك:

- لا تشارك معلومات بطاقتك الائتمانية مع أي شخصٍ آخر سوى الموقع الذي تريد إجراء عملية الدفع فيه. كما عليك التأكّد أنّ الموقع الإلكتروني لا يخزّن معلومات البطاقة لديه. تذكّر أنّه يجب ألّا تشارك تلك المعلومات معهم عبر البريد أو بشكل مكتوب مثلًا، بل عليك إدخاله من نموذج الدفع فقط وليس في مكانٍ آخر.
- لا تشارك فواتيرك الإلكترونية مع أي جهة غير مخوّلة فقد يكون بها معلوماتٌ حساسة.
- تأكّد من عنوان الويب الذي تقوم بإجراء المعاملة فيه وأنّه تابعٌ للموقع الإلكتروني الذي تريد الشراء منه (أي ليس موقعًا مزيّفًا).
- لا تجري عمليات الشراء والدفع على الإنترنت عبر شبكة اتصال لاسلكية عامّة (Public Wifi) لأنّها خطرة وقد يُكسر تشفيرها عبر هجماتٍ متعددة في هذا النوع من الشبكات. استعمل شبكاتك المنزلية أو شبكة 4G/5G فقط.
- عندما تنتهي من إجراء المعاملة انظر إلى حساب بطاقتك الائتمانية في البنك وتأكّد أنّ

المبلغ المقتطع هو نفسه المبلغ الذي من المفترض أن يحوِّلَه الموقع منك مقابل عملية الشراء (وليس أكبر منه مثلًا).

- إن حصلت مشكلة فأخبر البنك مباشرةً واتصل بالدعم الفني.

12. 3. خاتمة الفصل

إجراء المعاملات الآمنة على الإنترنت ليس بتلك الصعوبة كما ترى والموضوع ما هو إلّا بضع نصائح وتحذيرات ليأخذها المرء بالحسبان قبل أن يقدم على عمليات الدفع والشراء من مواقع لا يعرفها.

أمّا بخصوص سجل بطاقاتك الائتمانية (ما تشتريه عن طريقها) فللأسف لا يوجد طريقة لحماية نفسك ضد البنك منها، فالبنك سيظل يمتلك هذه المعلومات ولا يمكنك حذفها أو إخباره بعدم تخزينها مثلًا. فبمجرّد استخدامك للبطاقة الائتمانية أنت تتخلى عن حقّك في إخفاء مشترياتك وخصوصيتك أمام البنك.

13. تأمين الهاتف المحمول

إنّ تأمين الهاتف المحمول في هذا العصر ضرورة ملحّة وهذا لأنّ الكثير من الناس يقضي معظم وقته على هذه الهواتف. والهواتف هي أضعف نقطة أمان للمستخدمين فهي ليست مؤمّنة افتراضيًا بصورة جيّدة للأسف كما أنّ عملية تأمينها الحقيقية صعبة وفوق مستوى معظم المستخدمين العاديين، على عكس الحواسيب مثلًا.

سيشرح هذا الفصل كلّ ما يمكن أن يفيد المستخدم العادي لتأمين هواتفه المحمولة، وسنركّز على أنظمة أندرويد فهي الأكثر شيوعًا و90% من الناس يستخدمونها.

استخدمنا نظام أندرويد 6.0 في هذا الشرح، ورغم أنّه قديمٌ جدًا مقارنةً بأحدث الهواتف الصادرة مؤخّرًا إلّا أنّ ذلك مفيد فهذا يضمن أنّ جميع المزايا التي نتحدث عنها في هذا الكتاب ستكون موجودة في جميع إصدارات أندرويد التي صدرت بعد 6.0 وبالتالي تشمل معظم المستخدمين. قد تتغير مواضع الإعدادات وأمكنتها بناءً على إصدار نظام أندرويد المُستعمل بالإضافة إلى الشركة المصنّعة للهاتف المحمول، وقد تأتي إعداداتٌ جديدة من جوجل في الإصدارات الأحداث لإدارة الخصوصية لكن ثِقّ تمامًا أنّ هذه الميّزات موجودة في جميع إصدارات أندرويد ولا يُحذف منها شيء في الإصدارات الحديثة.

13. 1. لا يمكنك تأمين الهاتف المحمول

أو بالأصحّ لا يمكنك تأمين الهاتف المحمول بصورة كاملة.

يأتي الهاتف المحمول - سواءً كان من آبل أو سامسونج أو أيّ شركة - بالكثير من البرمجيات مغلقة المصدر افتراضيًا، بالإضافة إلى كون النظام نفسه غير قابل للاستبدال وإلّا ستخسر ضمان الشركة المصّنعة كما شرحنا في فصولٍ سابقة. هناك العشرات من البرمجيات التي تعمل على هاتفك

ولا تدري ماذا تفعل أو ما هي أو ما البيانات التي تجمعها عنك، وهي جزءٌ من نظام التشغيل نفسه الذي يأتي مسبقًا على الجهاز.

هذا بالإضافة إلى كون طبيعة الهواتف المحمولة غير قابلة للتأمين بصورة كاملة؛ شبكات الاتصال الخلوي مثلًا قادرة على تحديد موقعك الحالي حسب بعدك أو قربك من أبراج الاتصال الخاصّة بها، كما أنّ تعقّبك عبر نظام GPS (تحديد المواقع وفق الأقمار الاصطناعية) ممكن بسبب استخدامك لتطبيقات الخرائط (مثل خرائط جوجل)، وهذه أشياء منحصرة بالهواتف المحمولة دونًا عن الحواسيب لأنّك لا تستخدم حاسوبك مثلًا للتنقل في المدينة أو للاتصال بالآخرين، وبالتالي طبيعتهما مختلفة.

كما أنّ الكثير من الهواتف المحمولة تأتي بنظام أندرويد غير محدّث إلى آخر إصدار؛ وهو ما يعني نظريًا وجود العشرات من الثغرات الأمنية في هذه الهواتف، ولا يمكن تحديثها لآخر إصدار أندرويد حيث أنّ الشركات المصنّعة لا تحدّثها بعد مرور أول سنةٍ من إطلاقها في الغالب.

أضف إلى ذلك طبيعة استخدام الهواتف المحمولة، حيث يحمّل مستخدمو اليوم عشرات ومئات التطبيقات المختلفة على هواتفهم ليستخدموا مختلف الخدمات ومواقع الإنترنت، بينما لا يحصل هذا على الحواسيب مثلًا حيث يقضي المستخدم معظم وقته داخل متصفّح الويب فقط.

ولا يُنس صعوبة التعامل مع الهواتف المحمولة للعمليات الطويلة أو المعقّدة؛ فأنت بحاجة إلى الكثير من الضغط بإصبعك وإجراء العديد من الإجراءات لتأمين هاتفك وهذا أصعب للتحكّم ويأخذ وقتًا طويلًا لفعله، على عكس الحواسيب التي تأتي بفأرة ولوحة مفاتيح، وبالتالي يصبح المستخدمون أكثر كسلًا ورغبةً في ألّا يفعلوا شيئًا بالمرّة لتأمين أنفسهم.

تأتي أخيرًا مشكلة العتاد؛ فالكاميرا الأمامية والخلفية والميكروفون مدمجون في الهاتف نفسه ولا يمكن تعطيلهم فيزيائيًا، وبالتالي لا يوجد لديك ضمان أنّ هذه الكاميرا الأمامية التي تنظر إلى وجهك 24 ساعة لم يخترقها أحدهم في الواقع وهو ينظر إليك في هذه اللحظة ويسمع صوتك. وهذا مختلفٌ عن الوضع في الحواسيب حيث يمكنك تحريك الكاميرا بعيدًا (إن كانت منفصلة على USB) أو على الأقل تغطيتها بشريطٍ لاصق (لكن هل يمكنك تغطية كاميرا الهاتف بشريط لاصق؟).

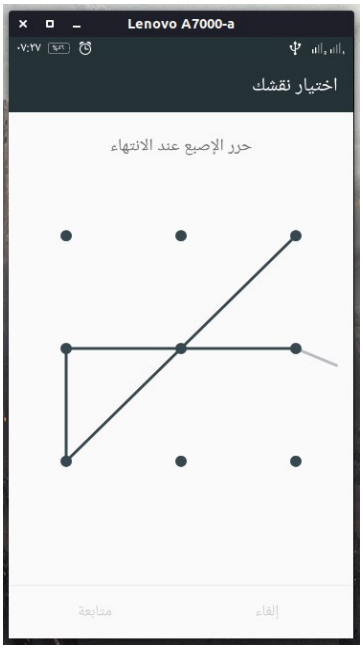
لكن ما لا يُدرك كلّه لا يُترك جلّه. سنحاول شرح أهم أساسيات الحفاظ على الخصوصية والأمان الرقمي على الهواتف المحمولة مما يمكن فعله بسهولة، وهذا أفضل للمستخدم من أن يترك نفسه عرضةً لكلّ شيءٍ يصيبه. لكن ضع في الحسبان أنّه في النهاية إن كنت تحاول تأمين نفسك ضد مزوّد خدمة الاتصال الخلوي أو أي جهة تتطلب مستوىً عالٍ من الحماية ضدها فحينها لن ينفعك

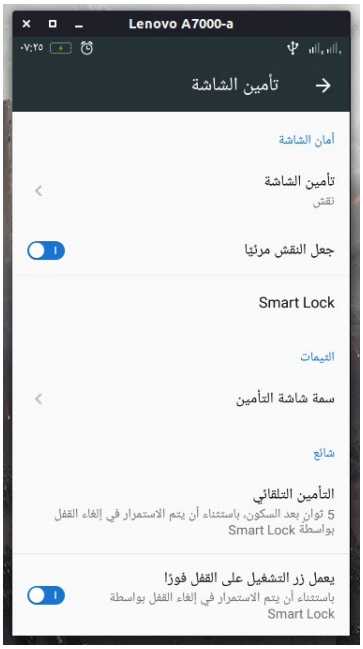
المذكور في هذا الكتاب، لكنّه ينفع لحماية نفسك من الاختراق والتطبيقات الخبيثة وما شابه ذلك، كما أنّ التشفير سيحمي بياناتك حتّى في حال السرقة مثلًا.

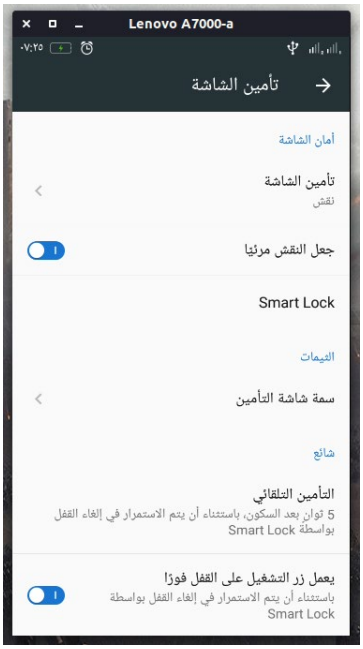
13. 2. تأمين الإعدادات الافتراضية

أوّل شيءٍ نحتاج فعله هو إنشاء قفل للشاشة (Screen Lock) لحماية الجهاز من العبث به إن وقع بأي المتطفلين أو السارقين (بصورة طفيفة للسارقين لكننا سنتبع هذا بالتشفير). وقفل الشاشة هو إمّا «نقش» (Pattern) ترسمه عند رغبتك بفتح الجهاز أو رقم أو كلمة مرور تدخلها عند رغبتك بفتحه، وبالتالي لا يمكن لأحدٍ سواك أن يفتح الجهاز ويصل إليه.

اذهب إلى الإعدادات (Settings) ---> تأمين الشاشة (Lock Screen) وستجد كلّ الإعدادات





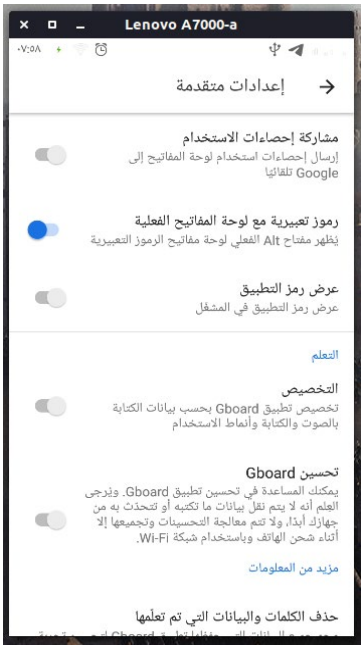


التي تحتاج إليها هنا. اضغط على «تأمين الشاشة» (Screen Lock) أمامك ثمّ اختر نوعيّة قفل الشاشة الذي تريده (نقش، رقم، كلمة مرور... إلخ) ثمّ ارسم النقش أو أدخل كلمة المرور التي تريدها.

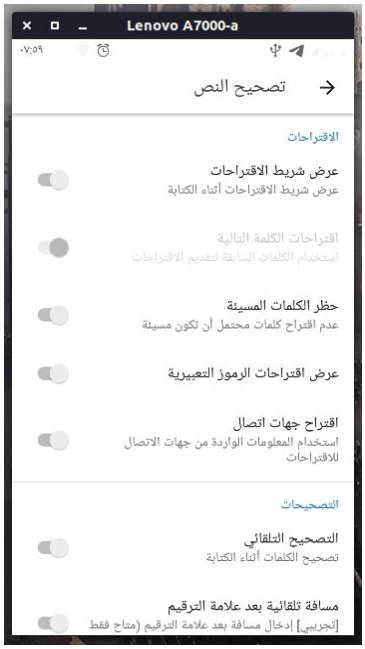
يمكننا الآن الشروع في تعطيل إعدادات مشاركة البيانات ومعلومات الأعطال مع الشركات المصنّعة للهواتف، وهذا لتجنّب رفع شيءٍ من بياناتنا إليها واستهلاك الشبكة. اذهب إلى «حول الهاتف» (About Phone) وعطّل إعدادات مشاركة البيانات من هناك:

كما عليك فتح تطبيق «Google» الذي يدير كامل حسابك في جوجل على الجهاز، ثمّ النقر على هذه النقطة الرأسية في أعلى يسار الشاشة ثمّ تعطيل «الاستخدام وبيانات التشخيص» (Usage & Diagnostics):

الشيء التالي لفعله هو تعطيل إظهار الإشعارات أثناء قفل الشاشة. إن أخذ أحدهم هاتفك مثلًا أو إن كنت تتصفحه بجانب أحدهم فستلاحظ ظهور كامل محتوى الرسائل والإشعارات المختلفة أثناء قفل الشاشة ولا نريد ذلك. يمكنك تعطيل هذه الميّزة من الإعدادات (Settings) --> مركز التنبيهات (Notifications Center) واختيار «عدم عرض إشعارات على الإطلاق»:



إنّ لوحة المفاتيح الافتراضية في أندرويد هي تطبيقٌ اسمه Gboard (وقد تكون غيرها على بعض الهواتف من بعض الشركات، لكن يمكنك تثبيتها على أي هاتف محمول أو اتباع نفس النصائح بصورة عامّة)، وهي لوحة المفاتيح الرسمية من جوجل لأنظمة أندرويد. هناك بعضٌ من إعدادات مشاركة البيانات التي عليك تعطيلها كذلك من إعدادات هذا التطبيق. يمكنك الوصول إلى إعدادات Gboard من الإعدادات (Settings) ---> اللغة والإدخال (Language & Input) ---> Gboard ---> إعدادات متقدّمة (Advanced Settings) ثمّ



عطّل خيارات «مشاركة إحصاءات الاستخدام» و«تحسين Gboard» و«التخصيص» كما بالصورة:

ومن نفس خيارات التطبيق اذهب إلى تصحيح النصّ (Text Correction) وعطّل «اقتراح جهات الاتصال» (Suggest Contacts) كما بالصورة:

علينا الآن مراجعة خدمات الموقع (Location Services) من الإعدادات ثمّ النظر فيها. إننا ننصح بتعطيل خدمات الموقع إلّا عند الحاجة لاستخدامها (مثل المشي مع خرائط جوجل مثلًا) وبالتالي تتخلص من تعقّب موقعك طيلة الوقت (باستثناء مزوّد الاتصال الخلوي، حيث سيظل قادرًا على تعقّبك). ستظهر لك في تلك الصفحة خدمات الموقع المفعّلة حاليًا ويمكنك الضغط على كلٍ منها ومراجعتها. إنّها غالبًا:

- خدمات تحديد مواقع الجغرافي في حالات الطوارئ: وهذا لتتمكن خدمات الطوارئ من معرفة موقعك في حال حصل مكروهٌ لك. يمكنك تفعيل أو تعطيل هذه الميّزة لكن لاحظ أنّ خدمات الطوارئ ستظل قادرةً - نظريًا - على معرفة موقعك عن طريق مزوّد الاتصال الخلوي.
- سجل المواقع الجغرافية في جوجل: عطّلناها مسبقًا في الفصول السابقة من حسابنا على جوجل. تأكّد من تعطيلها
- ميّزة مشاركة الموقع الجغرافي على جوجل: إن أردت مشاركة موقعك الجغرافي مع أحدهم، تأكّد من تعطيلها.

أخيرًا يمكنك تأمين بطاقات الاتصال (SIM Card) وهذا عبر طلب شِفرة سرّية تحفظها أنت عند إطفاء الجهاز وإعادة تشغيله، لا تضيف هذه الميّزة الكثير من الأمان لكنّ وجودها مهم لحماية بطاقة الاتصال من أن يستخدمها الآخرون. يمكنك الوصول إليها

من الإعدادات (Settings) --> الأمان (Security) --> إعدادات تأمين بطاقة SIM (Set up SIM Card Lock) ومن هناك يمكنك تغيير رقم التعريف الشخصي للبطاقة وكتابة رقم الأمان الذي تريده (تأكّد من حفظه وإلّا قد تخسر بطاقة الـSIM إلى الأبد إن نسيته):

13. 3. تأمين التطبيقات وصلاحيّاتها

التطبيقات وما أدراك ما التطبيقات، جبهة الحرب الأولى.

إنّ تأمين التطبيقات واستخدامها هو ثاني أصعب شيء على الهواتف المحمولة بعد محاولة تأمين نظام التشغيل نفسه، وهذا لأنّ كلّ تطبيقٍ تنزّله على الجهاز هو تطبيقٌ قد يكسر حمايته أو يخترقه، وبالتالي الكثير من الجهد والتعب المستمر في تأمين هذه التطبيقات ومراقبة نشاطها مطلوب.

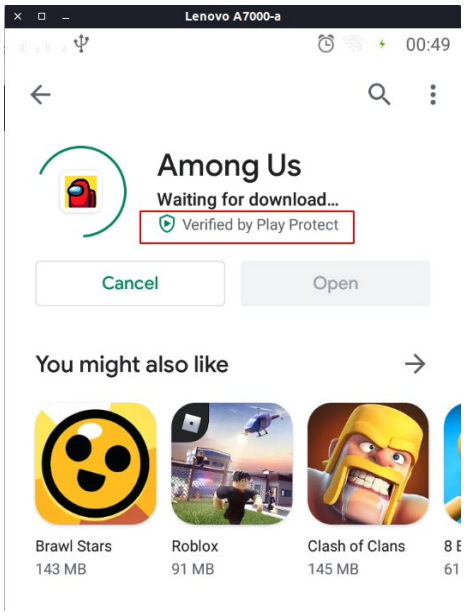
ينزّل معظم المستخدمين تطبيقاتهم من متجر جوجل بلاي (Google Play) الخاصّ بجوجل، فهو الذي يأتي افتراضيًا مع الجهاز كما أنّ جميع التطبيقات متوفّرة عليه، لكنّ هذا سيتطلب منك حسابًا على جوجل لتتمكن من استعماله، وبالتالي تدير جوجل جميع تطبيقاتك في الواقع عن طريق ما يُعرف بـGoogle Play Services.

لكنّ بعض المستخدمين لا يعجبهم ذلك ولا يريدون الارتباط بخدمات جوجل. وهؤلاء أنشؤوا متاجر تطبيقاتٍ بديلة ليستعملوها بدلًا من متجر تطبيقات جوجل للتخلّص من الحاجة إلى حساب جوجل فقط لتثبيت البرامج.

أشهر هذه المتاجر البديلة هو متجر F-Droid المجاني والمفتوح المصدر لأنظمة أندرويد وعليه حاليًا آلاف التطبيقات المتوفّرة جميعها مفتوحة المصدر، فالمتجر لا يقبل البرامج غير المفتوحة المصدر وبالتالي تغيب عنه جميع التطبيقات الأساسية الشهيرة، لكنّه مفيد لبرامج الأدوات (Utilities) وغير ذلك. يمكنك تثبيت المتجر على نظام الأندرويد الخاصّ بك وتنزيل ما يعجبك من التطبيقات المتوفّرة.

ومن المتاجر الجميلة كذلك متجر Aurora، وهو في الواقع متجرٌ مفتوح المصدر ينزّل البرامج مباشرةً من متجر جوجل بلاي لكن دون الحاجة لحساب جوجل أو واحدٍ من خدماتها (ودون الحاجة لاستخدام تطبيق متجر جوجل بلاي)، وبالتالي أنت تحمّل ملفّ الـAPK (ملفّ البرنامج التنفيذي) الخاصّ بالبرنامج مباشرةً ثمّ تثبّته على جهازك دون المرور بجوجل. وهذا ممتاز لأنّك ستصبح قادرًا على الحصول على جميع التطبيقات التي تريدها من متجر جوجل بلاي دون أي صعوبة تذكر. فقط ابحث عن اسم التطبيق الذي تريده في المتجر ويمكنك تحميله بعدها بنقرة زرّ. يريك المتجر كذلك

ما هي برمجيات التعقّب (Trackers) المُكتشفة في كلّ برنامج ويمتلك نظام حماية داخلي متطور.



إننا ننصح بشدّة بالاستغناء عن خدمات متجر جوجل بلاي واستخدام F-Droid وAurora لتحميل التطبيقات وإدارتها على هاتفك المحمول، فالأوّل يمكنه إحضار التطبيقات مفتوحة المصدر لك والثاني يمكنه تحميل كلّ التطبيقات الأخرى التي تحتاج إليها من جوجل بلاي (مثل تطبيقات البنوك أو التطبيقات المحلّية في بلدك وما شابه).

إن أبيت إلّا استعمال جوجل بلاي، فتأكّد أنّ التطبيقات التي تنزّلها لها تقييمات جيّدة (أكثر من 3.5 نجوم على الأقل) ولها أكثر من 50 ألف تحميل. انظر أثناء تنزيلك للتطبيق إلى أعلى الصفحة وقد تجد إشارة اسمها «Verified by Play Protect» وهي تعني أنّ هذا التطبيق قد فُحص من طرف جوجل [1] للكشف عن البرمجيات الخبيثة ولم يوجد به ما يثير الشكوك (وجوجل لا توفّر هذا كضمان أنّه خالٍ 100% منها، لكنها طبقة حماية إضافية). تثبيتك لهذه التطبيقات أفضل بكثير من تثبيتك لغيرها:

كلّ ما سبق متعلّقٌ بمصادر التطبيقات، أمّا إن أردنا التحدّث عن التطبيقات نفسها فعلينا حتمًا ذِكر الصلاحيات أو الأذونات (Permissions) التي قد تتمتع بها هذه التطبيقات. الصلاحيات هي ببساطة إمكانية برنامجٍ معيّن بالوصول إلى بعض المزايا المتوفّرة في العتاد أو نظام التشغيل، ويمكن للمستخدم عبر نظام التشغيل منح أو منع هذه الصلاحيات وإدارتها كيفما شاء.

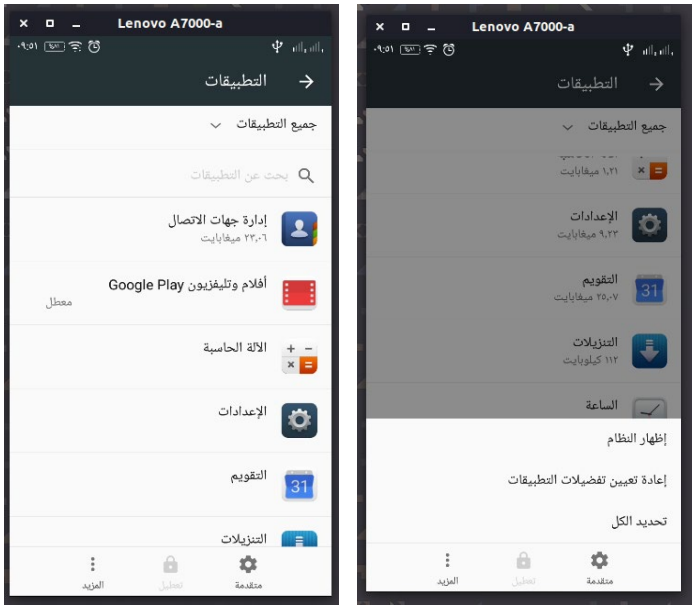
الصلاحيات ميّزة مهمّة جدًا على الهواتف المحمولة وهي لبّ الأمان الرقمي عليه؛ ذلك أنّ البرامج التي تثبّتها على جهازك ستطلب منك قبل التثبيت صلاحياتٍ معيّنة (كالوصول إلى الميكروفون أو الكاميرا أو الصور أو وسائط التخزين ...إلخ) وأنت من عليه أن يقرر إن كانت تلك الصلاحيات يحتاج إليها التطبيق بالفعل ليعمل أم لا.

فمثلًا إذا كنت تبحث عن تطبيقات الآلة الحاسبة في متجر التطبيقات وعند تثبيت أحدها وجدته يطلب الوصول إلى الكاميرا أو الميكروفون أو الصور الخاصّة بك فهذا تطبيقٌ مشبوه حينها، لأنّ الآلة الحاسبة - المفترض - أنّها لا تحتاج هذه الصلاحيات لتعمل فلماذا يطلبها هذا التطبيق منك؟ هذا يعني أنّه يفعل أشياءً يجب ألّا يفعلها على نظامك.

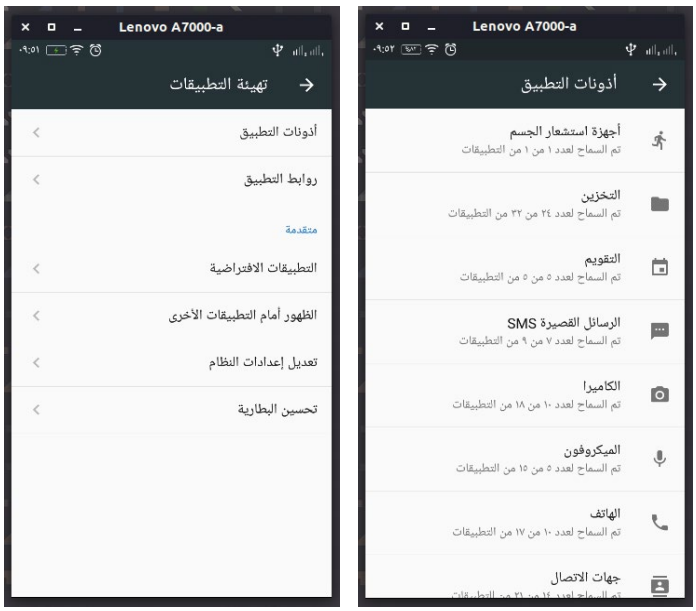
عليك تجنّب تثبيت التطبيقات التي تطلب صلاحياتٍ موسّعة لا تحتاج إليها من هذا النوع،

وكلّ تطبيقٍ تشكّ فيه أنّه يطلب صلاحياتٍ لا يحتاج إليها لا تثبّته. أو إن أردت فيمكنك تثبيته ثمّ إلغاء صلاحياته الموسّعة من إعدادات التطبيقات مباشرةً بعد تثبيته (وقبل فتحه لأوّل مرّة) كما سنشرح الآن:

يمكنك رؤية جميع التطبيقات المثبّتة على جهازك من الإعدادات (Settings) --> التطبيقات (Apps). كما يمكنك النقر على زرّ المزيد (More) وإظهار تطبيقات النظام لرؤيتها جميعًا:



إن ضغطت على زرّ متقدّمة (Advanced) فستصل إلى بعض الإعدادات المخفية المتعلّقة بإدارة التطبيقات، ويمكنك الضغط على أذونات التطبيق (App Permissions) لرؤية جميع الصلاحيات الحالية على الجهاز بالإضافة إلى كلّ التطبيقات التي تستعمل تلك الأذونات مفصّلةً إلى تصنيفاتٍ مختلفة:



عليك تصفّح جميع هذه الصلاحيات وتعطيل أيّ تطبيقٍ مشبوه ترى أنّه يجب ألّا يمتلك تلك الصلاحيات. كما يمكنك مثلًا تثبيت التطبيقات التي تطلب منك صلاحياتٍ كثيرة ثمّ بعد التثبيت تعطّلها أنت من هذه الخيارات.

من المنصوح كذلك استخدام برنامج مضاد فيروسات ويمكنك العثور على الكثير منها وتجريبها من متجر التطبيقات الخاصّ بك. ولطبيعة عملها والمنافسة الشديدة بينها فهي ليست مفتوحة المصدر للأسف لكنّ وجودها ضروري لتأمين هاتفك وحمايته من الأخطار، ولن نتمكّن من الإشارة إلى أسماءً معيّنة في هذا الكتاب بسبب ذلك.

ننصح أخيرًا باستعمال إصدار الويب من التطبيقات الشهيرة بدلًا عن تطبيقاتها للهواتف المحمولة. مثلًا بدلًا من استعمال تطبيق فيسبوك، احذفه من جهازك بالكامل وتصفّح فيسبوك عن طريق متصفّح الويب فقط على الرابط facebook.com، وكذا بالنسبة لتويتر ويوتيوب وغيرهم من الخدمات.

وهذا لأنّ كل تطبيقٍ جديد تضيفه إلى هاتفك المحمول هو نقطة هجوم ممكنة على أمانك أو خصوصيتك، فهذه التطبيقات تمتلك افتراضيًا العشرات من الصلاحيات المفعّلة على جهازك وهي قادرة بالتالي على جمع ما تشاء من معلومات، وهي مرتبطة بالخدمات الأخرى من تلك الشركات (مثلًا فيسبوك قد يتشارك ببعض البيانات مع واتساب، ويوتيوب يشارك بعض البيانات مع خدمات جوجل الأخرى). بينما إن حذفتها واستعملت تلك الخدمات عبر متصفح الويب فقط فستصبح تلك الخدمات مقيّدة بصلاحيات متصفح الويب، ولن تتمكن من العمل خارجه، وسيخبرك متصفح الويب ما قد تحتاجه هذه المواقع منك بالضبط من بيانات.

يمتلك كلٌ من متصفحيّ فيرفكس وBrave إصداراتٍ مختلفة للهواتف الذكية، ويمكنك تثبيتهما على جهازك للتمتع بتصفّحٍ أكثر أمانًا وخصوصية من المتصفحات الافتراضية على نظام التشغيل الافتراضي للهاتف المحمول.

13. 4. حذف الملفات بصورة نهائية

كما شرحنا في فصولٍ سابقة فإنّ الملفّات لا تُحذف نهائيًا عند حذفها من الأقراص الصلبة أو بطاقات SD، بل تبقى محتوياتها موجودةً على القرص حتّى تأتي بياناتٌ جديدة صدفةً وتستبدلها. وهذه مشكلة إن أردت بيع هاتفك أو استبداله أو إعطاءه لشخصٍ آخر لأنّه يمكنه استعمال برامج استعادة الملفّات لاسترجاع ملفّاتك وبياناتك الشخصية المحذوفة. حتّى ضبط الجهاز على وضع

المصنع (Factory Reset) لن يحميك من ذلك. يمكنك مراجعة الأوراق البحثية [1] [2] لرؤية التفاصيل وأسباب ذلك.

لاحظ أنّه هناك عدّة أنماط للتخلّص من البيانات المحذوفة وحذفها للأبد:

- تشفير تلك البيانات وبالتالي منع الوصول لها من قبل الآخرين حتّى عند استرجاعها، هذه الطريقة هي الأقوى (ولهذا دومًا ننصح بالتشفير في كلّ أجزاء هذا الكتاب) لكنّها مع ذلك عرضة لهجمات استرجاع ملفّ التشفير نفسه (Encryption Key Restoration) وبالتالي يُمكن كسرها نظريًا إن كان يركض وراءك أحد ما، لكن أبو عبّود مصلّح الهواتف والحواسيب في حيّكم يستحيل عليه ذلك.
- الكتابة فوق كامل القرص الصلب أو بطاقة SD، وهذا حلٌ فعّال لأنّه يكتب فوق كامل البيانات على القرص وليس فقط استهدافًا لملفّات معيّنة.
- الكتابة فوق المساحة الحرّة فقط من القرص الصلب أو بطاقة SD. وهذا مناسب إن كنت تريد التخلّص من كلّ شيءٍ حذفته في الماضي على تلك الأقراص لكن دون أن تحذف شيئًا جديدًا من بياناتك الحالية.
- الكتابة عدّة مرّات فوق ملفّ معيّن وهذا هو الخيار الأشهر والأسهل لكنّه الأكثر عرضةً للضعف كذلك، لأنّه على المستخدم الكتابة مرّاتٍ كثيرة فوق الملفّ ويستخدم تقنياتٍ معيّنة ليكون فعّالًا ومعظم برامج الحذف النهائي في الواقع ليست بتلك الفاعلية.

إنّ عملية الكتابة فوق البيانات المحذوفة لا تعني بالضرورة حذف البيانات وهذا يعتمد على عوامل المساحة والطريقة المُستعملة بالإضافة إلى بعضٍ من العشوائية. وبالتالي من الواجب إجراء عدّة «مسحات» أو عمليات كتابة فوق البيانات (Pass) لزيادة فرصة حذفها للأبد، أمّا المسحة الواحدة فلا تفيد في شيء غالبًا (إلّا إن كانت الطريقة مصممة بالأساس لأقراص SSD وSD Cards فحينها الوضع يختلف ويمكن بمسحة واحدة).

كما ترى فإجراء المسحات نفسها يتم بطرق مختلفة ولها معاييرها الخاصّة التي تحتاج الكثير من الأبحاث وهي معقّدة. لكن نريد الإشارة إلى أنّ الحذف النهائي حاليًا وفق آخر ما توصّل له المجال (State-of-the-Art) هو طريقة NIST 800-88. وهي مصممة خصيصًا لأقراص SDD وبطاقات SD وفلاشات USB الشبيهة وبالتالي تكتفي بمسحة واحدة، أمّا الطرق الأخرى مثل DoD 5220.22-M فهي غير مصممة لذلك وبالتالي تحتاج 7 مسحات. إننا ننصح بقراءة المقال [3] للمزيد من المعلومات عن معايير تدمير البيانات بصورة نهائية.

والمشكلة الحقيقية هي أنّه لا توجد برامج مفتوحة المصدر للأسف على الهواتف المحمولة للقيام بالمهمّة بصورة فعّالة، وبالتالي يضطر المرء لاستعمال برامج مغلقة المصدر أو مدفوعة لأداء ذلك. عليك البحث بنفسك عن برامج تدعم طرق الحذف السابق ذكرها على أجهزتك. برنامج iShredder على أندرويد قد يكون واحدًا منها.

13. 5. التشفير على الهاتف المحمول

تشفير الملفّات مهم جدًا لحمايتها من الوصول في حال السرقة أو الاختراق مثلًا. ولحسن الحظّ فإنّ التشفير مدعومٌ من نظام أندرويد نفسه ويمكنك تفعيله بسهولة.

من الإعدادات (Settings) --> الأمان (Security) انقر على التشفير (Encryption). وستتم عملية التشفير في غضون نحو ساعة أو أكثر من ذلك اعتمادًا على حجم بياناتك. ستُستعمل كلمة المرور أو نقش الشاشة الذين ضبطتهما بالفعل لإلغاء تشفير الجهاز:

هناك كذلك العشرات من التطبيقات مفتوحة المصدر على متجر F-Droid لمختلف مهام التشفير؛ تشفير ملفّات معيّنة أو تشفير الرسائل أو التحقق من تشفير القرص أو إرسال الرسائل المشفّرة وغير ذلك الكثير. يمكنك تصفّحها وتثبيت ما يعجبك منها فكلّها مجانية ومفتوحة المصدر.

لا تنس استخدام Cryptomator - البرنامج الذي شرحناه في فصل التشفير - لتشفير مساحة التخزين السحابية كـGoogle Drive وDropbox، وهو يعمل كذلك على أنظمة أندرويد وiOS.

13. 6. أنظمة بديلة لهواتف الأندرويد

إن نظام أندرويد مبني على نواة لينكس، والكثير من أجزائه مفتوحة المصدر مما يسمح للمطورين ببناء توزيعاتٍ مختلفة منه وإعادة توزيعها للناس بما يناسب احتياجاتهم. هناك مجتمعات هائلة من المطورين والمستخدمين حول ما يُعرف بـ«الرومات» (ROMs) الخاصّة بالأندرويد وهذه الرومات غالبًا ما تكون خاليةً من منتجات جوجل وخدمات تعقّبها وبالتالي هي أأمن وأفضل للاستخدام. هناك أنظمة تشغيل أخرى كذلك غير أندرويد يمكن تثبيتها على الهواتف المحمولة.

إن كنتَ مستعدًا لصرف عدة أيام من وقتك لاستبدال نظام الأندرويد الموجود على جهازك بنسخة أخرى مبنية عليه وإن كنت مستعدًا كذلك لخسارة ضمان الجهاز في سبيل أمانك وخصوصيتك، فيمكنك الاطلاع حينها على المشاريع التالية:

- LineageOS: توزيعة مجانية ومفتوحة المصدر من أندرويد للهواتف المحمولة، تركّز على حذف تطبيقات جوجل افتراضيًا والاهتمام بالخصوصية.
- /e/OS: توزيعة مبنية على الأندرويد للمهتمين بأقصى خصوصية افتراضيًا وتوفير خدمات بديل لكل خدمات جوجل. يمتلكون كذلك هواتف مسبقة الشحن بنظامهم المفتوح المصدر.
- Ubuntu Touch: توزيعة مبنية على أوبونتو وليس أندرويد، مما يجعلها لا تعمل على معظم الهواتف سوى الحديثة والقوية منها لكنّ هذا يجعلها أفضل من غيرها بكثير (باستثناء كون الاتصالات الخلوية لا تعمل عليها في كلّ المناطق).

انتبه كذلك إلى أنّ الأنظمة مثل البرامج؛ قد تكون محملة ببرمجيات تجسس واختراق وتعقّب كذلك، ويجب ألّا تحمّلها من أي مصدر مشبوه أو غير موثوق.

من الواجب الانتباه كذلك عند التعامل مع مصلّحي الهواتف المحمولة المحليين في مدينتك أنّهم قد يكونون غير موثوقين أو غير متعلمين بصورة كافية، فيحمّلون أنظمة (رومات) من مصادر مشبوهة إمّا عن علم أو جهل ويثبّتونها لك دون علمك. فالقصد أنّ الثقة عامل أساسي جدًا هنا.

لا تسلّم هاتفك المحمول إلّا لمن تثق به!

13. 7. خاتمة الفصل

قد تستغرق عملية تأمين الهاتف المحمول الكثير من الوقت والجهد إلّا إنّ النتائج ستكون أفضل بكثير من أن تُخترق أجهزتك وتُسرّب بياناتك، ولهذا من المهم اتباع الإجراءات السابقة لضمان عدم حصول ذلك.

لا تنس كذلك أنّ هذه النصائح ليست شاملة لكل شيءٍ متعلّق بالهاتف المحمول فكما ذكرنا لا يمكن تأمين الهاتف بمحمول بصورة كاملة، لكنّها تغطّي معظم المواضيع المهمّة للقارئ العادي.

14. كيف تعرف أنك اخترقت وماذا تفعل عندما يخترقونك؟

معرفة ما إذا كنتَ مُخترَقًا أم لا هو من أهم الأشياء التي عليك فعلها لضمان أمانك الرقمي، فقد تكون مُخترقًا بالفعل وعلى أكثر من مكان دون أن تشعر بذلك. سيشرح هذا الفصل كيفية معرفة ذلك بالإضافة إلى نصائح لفعلها ما إذا اكتشفت أنّك مُخترق بالفعل سواءً في الخدمات التي تستعملها أو الأجهزة التي تستعملها كالحواسيب والهواتف المحمولة.

14. 1. كيف تعرف أنك مخترق أم لا؟

دعنا نوضّح في البداية أن «الاختراق» درجات وليس درجةً واحدة، فاختراق حسابك على فيس بوك ليس مماثلًا لاختراق كامل نظام التشغيل الخاصّ بك، واختراق بريدك الإلكتروني لا يساوي اختراق أحد حساباتك على مواقع التواصل الاجتماعي، كما أنّ وجود بعض البرمجيات الغريبة فجأة على نظامك أو ظهور بعض النوافذ المنبثقة لا يعني بالضرورة أنّ أحدهم قد اخترق كامل جهازك.

على سبيل المثال وكتجربة شخصية، قمتُ يومًا ما بتنزيل التطبيق الرسمي لأحد مشغّلي خدمات الاتصال الخليوي في أحد البلدان، ثمّ تفاجأت بعد فترة بإشعارات غريبة من نوعية: «أنا مهتمةٌ بك، تعال وحمّل هذه اللعبة»، وكان هذا غريبًا بالنسبة لي فالتطبيق رسمي من الشركة المركزية للاتصال الخليوي في ذاك البلد ويستعمله الملايين وكنتُ مستبعدًا أن ينحطّوا إلى هذا المستوى.

لكن هل هذا يعني أنّهم اخترقوا هاتفي المحمول بالكامل الآن وبالتالي عليّ حذف كل شيء؟ لا، فبعد تحليل الوضع تبيّن أنّها مجرّد خدمة دفع إشعارات (Push Notifications) كانت مُرفقة مع التطبيق الرسمي لتلك الشركة لا أكثر ولا أقل، أي أنّها تعرض هذه الإشعارات المزعجة فقط كنوع من الإعلانات للألعاب والبرامج التي يتعاقدون معها، لكنّها لا تسرق أو تحمّل أي بياناتٍ من الجهاز.

لكن كيف ستعرف أنت - كقارئ عادي - هذا وكيف ستفرّق بين هذا النوع من «الاختراق» وبين الاختراق الحقيقي لأجهزتك؟ العملية صعبة في الواقع وتحتاج الكثير من الوعي والتمرّس. لكن إليك هذه النصائح:

- إذا ثبّت برنامجًا من مصدرٍ موثوق أو عالي الموثوقية، كالتطبيقات الرسمية للبنوك أو الشركات الضخمة في بلدك ثمّ تفاجأت بسلوكٍ غريب على أجهزتك فقد تكون هذه التطبيقات هي سببها، وقد لا يعني بالضرورة أنّها قد سَببت اختراقك بالكامل بل قد تُسبب ذاك السلوك غير المعتاد فقط - مهما كان نوعه - وهنا يمكنك الارتياح أكثر. فقط تواصل مع المتخصصين في المجال - سواءً على المنتديات أو منصّات الأسئلة والأجوبة وغيرها - وأخبرهم بما حصل وهم سيساعدونك على التأكّد من الموضوع.
- إذا ثبّت برنامجًا من مصدرٍ مجهول، كمدوّنات الإنترنت أو المواقع التي لا تعرفها وحصل سلوكٌ غريبٌ في النظام - مهما كان صغيرًا - مثل تثبيت برمجيات لم تقم أنت بتثبيتها أو ظهور إعلانات ونوافذ منبثقة وما شابه، فهذا أدعى للقلق وأكثر قربًا من أن يكون اختراقًا حقيقيًا لكامل نظامك، وعليك قطع الإنترنت عن الجهاز والتواصل مع متخصص فورًا.
- إذا تغيّر متصفّح الويب الافتراضي لك أو تغيّر محرّك البحث الافتراضي دون علمك، فقد تكون بعض البرمجيات أو الإضافات التي حمّلتها هي من تسبب بذلك. لا تحتاج الكثير من القلق هنا لكن تحتاج البحث وراء الموضوع ولماذا حصل فجأة. مثلًا متصفّح فيرفكس في روسيا (وتركيا كذلك) يقوم تلقائيًا من فترة لأخرى بتغيير محرّك البحث الافتراضي إلى ياندكس Yandex وهذه صفقة بين مطوّري فيرفكس وياندكس لجعلهم يكسبون المال [1]، وهو تغيير رسمي حقيقي وليس شيئًا مشبوهًا من طرفٍ ثالث. لكن من الواجب عليك كمستخدم التحقق من ذلك بنفسك بالطبع وألّا تتجاهل الموضوع.
- إذا حصل بطءٌ مفاجئ في نظام التشغيل - سواءً للهاتف المحمول أو الحاسوب - وتكرر عدة مرّات دون أي سابق إنذار أو تثبيتك أنت لبرمجيات إضافية أو أي إجراءٍ من طرفك، فقد تكون هذه علامةً على اختراق جهازك وستحتاج أخذه إلى الصيانة لتتأكد من ذلك. لكن غالبًا ما يكون ضعف العتاد مع تقدّم عمره هو السبب في ذلك وليس عملية اختراق.
- إذا رأيت نوافذ منبثقة أو إشعاراتٍ إعلانية فهذا يعني أنّ بعض البرمجيات التي ثبّتها قد احتوت على ما يُعرف بالبرامج الإعلانية (Adware)، وقد تكون خبيثةً (تخرّب الجهاز أو تسرق منه بيانات) أو قد تكون مجرّد وسيلة لعرض الإعلانات لا أكثر ولا أقل. عليك فحص جهازك

بالكامل للتأكّد من الموضوع أو الاتصال بمتخصص. هناك برامج متخصصة كذلك في إزالة هذه البرامج والإشعارات الإعلانية.

- تمتلك مواقع الويب الشهيرة والخدمات الحساسة (مثل خدمات البنوك) سِجلًا بعمليات تسجيل الدخول إلى الحسابات، ويحتوي ذاك السجل على عنوان الآي بي لآخر عمليات تسجيل الدخول بالإضافة إلى الجهاز المُستعمل في ذلك (يمكنك رؤيته من الإعدادات) وآخر محاولات تسجيل الدخول الفاشلة. إذا تحققت منه يومًا ما ووجدت عنوان آي بي مختلف عن عنوان الآي بي الخاصّ بك (من غير دولة مثلًا) وبنظام تشغيل أو متصفّح لا تستعمله فمن المؤكّد هنا أنّ حسابك قد اختُرِق. كما إذا وجدتَ الكثير من محاولات تسجيل الدخول الفاشلة لحسابك فهذا يعني أنّ أحدهم كان يحاول اختراقك. لكن لاحظ أنّ مزوّد خدمة الإنترنت الخاصّ بك قد يغيّر عنوان الآي بي الخاصّ بك من طرفه فعنوان الآي بي الخاص بمشتركي مزوّدات خدمة الإنترنت غير ثابت (Non-static IP Address) عادةً لكن يجب أن يكون دومًا يشير إلى نفس الدولة (فإذا كان من دولة خارجية فهذا يعني أنك مُخترَق بغض النظر عن التفاصيل)، ولذا عليك التحقق من الموضوع أكثر. مثلًا افحص عنوان الآي بي الخاص بك في كلّ يوم وانظر إلى نتائج الاختبار بعد فترة شهر، من المفترض الآن ألّا تحصل أيّ عملية تسجيل دخول إلى حساباتك من خارج قائمة عناوين الآي بي هذه.
- استخدام برمجيات التنظيف (Cleaning Software) وبرمجيات مكافحة الفيروسات والحماية (Security & Anti-virus Software) على الهواتف المحمولة للتحقق من أمان أجهزتك. الكثير منها مجاني ومُستعمل من طرف ملايين الناس، ولا يمكننا أن ننصح بواحدٍ منها بالتحديد هنا لطبيعة هذه البرمجيات وتغيّرها باستمرار وكون معظمها مغلقة المصدر.
- إذا حصل أي نشاط للبيانات دون علمك، مثل إرسال رسائل البريد الإلكتروني أو نشر رسائل ومنشورات التواصل الاجتماعي أو نسخ وحذف الملفّات أو أي عملية متعلقة ببياناتك دون أن تقوم أنت بتنفيذها فمن المؤكّد أنّك قد اختُرقت.
- إذا كنتُ تستعمل برنامجًا مضادًا للفيروسات واكتشفت وجود فيروس خبيث لفترةٍ طويلة على جهازك فهذا يعني أنّك قد تكون مخترقًا طيلة تلك الفترة، لكن نوعية تلك الفيروسات وما كانت تفعله على حاسوبك هو مجالٌ للأخذ والردّ.
- إذا كان جهازك (سواء هاتف أو حاسوب) يمتلك كاميرا ورأيت ضوء الفلاش (Flash) الخاصّ بها قد اشتغل فجأة فمن المؤكّد هنا أنّك مُختَرق وبحاجة لفصل الكاميرا والميكروفون فورًا

(على الهواتف إمّا عطّل وصول جميع التطبيقات إليهما من الأذونات أو أطفئ الجهاز). ننصح دومًا بوضع الميكروفون بعيدًا عنك بالإضافة إلى إغلاق الكاميرا بشريطٍ لاصق وإزالته فقط عندما تستعملها.

14. 2. ماذا تفعل عندما يخترقون أجهزتك؟

حسنًا إذا، وقعت الكارثة واخترقوا حاسوبك أو هاتفك المحمول (اختراق كامل حقيقي).

عليك في البداية أن تهدأ وتحاول استجماع أكبر قدرٍ ممكن من تركيزك ووعيك فالخطوات التالية لِما بعد عملية الاختراق مهمة جدًا في محاولة تدارك ما يمكن تداركه من بياناتك وملفّاتك، طالما أننا نتحدث هنا عن اختراق حقيقي وليس فقط اشتباهًا.

عليك أن تحدد أوّلًا مالذي اختُرق بالضبط في أجهزتك (هل نزّلت لعبة فحصل الاختراق، هل حمّلت ملفًا فحصل الاختراق، هل فتحت رسالة فحصل الاختراق أم كيف)؟ وهذه الأجهزة التي اختُرقت، ما البيانات الموجودة عليها حاليًا وفي أي حالة (ملفّات، كلمات مرور محفوظة، تطبيقات اجتماعية، تطبيقات بريد إلكتروني، تطبيقات بنكية، حسابات بطاقات ائتمانية... إلخ)؟ هل ملفّاتك وبياناتك وبرامجك ما تزال هناك أمّ حُذفت وشفّرت الآن؟

عليك أن تعتبر أنّه بمجرّد تمكّن المُختَرِق (Hacker) من الوصول إلى جهازك ولو فترة بسيطة فحينها لديه وصولٌ كامل - وما يزال مستمرًا - عليها إلى اللحظة، وبالتالي لديه وصولٌ لكل شيءٍ مخزّن على تلك الأجهزة بما في ذلك الحسابات والخدمات التي تستعملها (يُستثنى من ذلك الملفّات ضمن خزنة شخصية مشفّرة بكلمة مرور منفصلة).

يُمكن اختصار معظم محتويات هذا الفصل في جملةٍ واحدة: افهم ماذا حدث وهل ملفّاتك ما تزال موجودة أم لا (دقيقة أو دقيقتين كحد أقصى)، وأطفئ الجهاز فورًا (ليس عن طريق نظام التشغيل، بل عن طريق زرّ الطاقة للحواسيب المحمولة وسحب شريط الكهرباء للحواسيب المكتبية، قطع مباشر فوري) ثمّ اطلب المساعدة من المتخصصين.

وهذا لأنّه بما أنّ المخترق قد تمكّن من الوصول إلى الجهاز فحينها لا ضمان لديك أنّه لا يزال يسحب المزيد من بياناتك وصورك وملفّاتك عبر الاتصال الشبكي الموجود في الجهاز، ولا تضمن مثلًا أنّه يشغّل - الآن - عملية تشفير لكامل قرصك الصلب لابتزازك به مقابل المال لاحقًا (فيروس الفدية Ransomware)، كما لا تضمن أنه ما يزال يحاول فعل أي شيءٍ آخر على الجهاز (حذف الملفّات كلّها، نسخها، تخريب نظام التشغيل، تخريب العتاد عبر ثغرة في الـBIOS... إلخ)، وبالتالي إطفاء الجهاز وقطع الاتصال بالكامل بينه وبين المخترق هو الخيار الأمثل لك حاليًا.

ولا تنحصر المشكلة بالاتصال الشبكي؛ لأنّه يكفيه أثناء فترة وصوله إلى الجهاز أن يدفع إليه ملفًّا تنفيذيًا (Script) يقوم لوحده بتشفير وحذف وتخريب الجهاز دون أي اتصالٍ بالشبكة. وبالتالي قطع الطاقة وإيقاف كلّ شيء عن العمل والمحافظة على الحالة الحالية للبيانات والملفّات هو الخيار الأمثل.

حسنًا، فصلت الجهاز الآن وقطعت عنه الطاقة. الآن عليك أن تأخذه إلى متخصص في مدينتك لهذا النوع من المشاكل وهو - المفترض - أن يخبرك بما يجب فعله بعدها.

إننا لا ننصح بمحاولة «محاربة» عملية الاختراق بنفسك لأنّها عملية متقدمة وطويلة ومعقّدة وتعتمد على عوامل عملية الاختراق نفسها، وليست شيئًا يُمكن تعليمه لأيٍ كان. فمثلًا إذا كان المُخترق قد قام بحذف ملفّاتك من على حاسوبك فحينها ما يزال هناك فرصة لاسترجاعها عبر برامج استعادة البيانات بل يمكن حتّى محاولة استعادة بعضٍ منها من الذاكرة العشوائية (RAM) إن كانت هناك، بل يمكن حتّى رؤية البرنامج الخبيث نفسه يعمل على الجهاز وهو في حالته الأخيرة من هناك. لكن عملياتك أنت على الجهاز قد تقضي على تلك الفرصة بالكامل وهذا لأنّ هذه البيانات المحذوفة قد تضيع مع أوّل عملية كتابة جديدة على القرص أو الذاكرة.

أضف إلى ذلك أنّ المُختَرِق قد يكون ترك برامج خبيثة متعددة بناءً على الإجراءات التي تعملها عليه؛ كأن يقوم تلقائيًا بتشفير وحذف كامل الملفّات في حال فتح برنامج معيّن أو ما شابه. ولهذا فإنّه لا فرصة لديك - كشخص غير متخصص - في هذه المواجهة بتاتًا.

لكن قد لا يمتلك الجميع إمكانية الوصول إلى متخصص في الحماية والأمان الرقمي لمحاولة حلّ المشكلة، وبالتالي يضطرون للتعامل معها على أيّةِ حال. لهؤلاء نقدّم النصائح المبدئية التالية في هذا الكتاب، ولكن نرجو استنفاذ كلّ ما يمكن في محاولة الوصول إلى متخصص قبل أن تحاول ذلك بنفسك.

قبل ذلك: سواءً اختُرق حاسوبك أو هاتفك المحمول، قم فورًا بتغيير كلّ بيانات وكلمات المرور المتعلّقة بالحسابات الموجودة على ذلك الجهاز (من مكانٍ آخر وليس نفس الجهاز)؛ إذا كان لديك تطبيقات بنكية مفتوحة مثلًا أو ربطت الجهاز بحساب Dropbox أو Google Drive، أو استعملت عليه فيس بوك أو تويتر أو خدمات جوجل ...إلخ، فغيّر كلمات المرور لكل تلك الحسابات فورًا. كلّ خدمة استخدمتها عبر ذاك الجهاز غيّر كلمة مرورها فورًا.

وتحقق بعدها من أجهزة الآخرين الموجودين معك ضمن الشبكة؛ فإذا اختُرق حاسوبك أنت فمن غير المستبعد أن يكون حاسوب الأفراد الآخرين من أسرتك على نفس الشبكة قد اخترقوا هم أيضًا، فافحص أجهزتهم لتعرف حالتها الحالية.

14. 3. ما تفعله عند اختراق الحاسوب

حدد أوّلًا ما هي البيانات المهمّة على الحاسوب لديك؟ هل لديك مشكلة في حذف كامل الملفات والبيانات أم أنت فعلًا بحاجة إليها؟ هل لديك نسخة احتياطية في مكانٍ ما أم لا تمتلكها؟ كذلك في آخر مرّة رأيت فيها الحاسوب يعمل، هل كانت ملفّاتك وصورك وبياناتك وبرامجك هناك كلّها أم رأيت أنّها قد حُذفت أو شُفّرت؟

إن كان لا يوجد لديك مشكلة في خسارة كامل البيانات:

- لا تستعمل الحاسوب حاليًا بتاتًا ولا حتّى مرّة واحدة.
- حضّر فلاشة USB - من حاسوبٍ آخر - عليها نظام لينكس، ثمّ أقلع منها بعد إدخالها في الحاسوب، واستعملها لحذف كامل الأقراص الصلبة وكامل البيانات الموجودة، ثمّ ثبّت النظام (سواءٌ لينكس أو ويندوز) من جديد من الصفر.
- تجنّب تثبيت أيّ شيءٍ تشتبه أنه هو السبب في الاختراق الأخير الذي حصل لك.

إن كان لديك مشكلة في خسارة البيانات، وتحتاج بالفعل الوصول إليها:

- قبل إطفاء الحاسوب، هل كانت ملفّاتك وبياناتك موجودة هناك عندما تحققت من ذلك أم لا؟ إن كان الجواب لا فحينها للأسف لا يوجد شيءٌ لتفعله حاليًا من طرفك وأنت مضطر للتواصل مع المتخصصين لإيجاد حلّ، وإن كان الجواب نعم فتابع القراءة.
- عليك تجنّب الإقلاع إلى نظام التشغيل المثبّت على الحاسوب مهما حصل. وبالتالي عليك تحضير فلاشة USB بنظام لينكس ثمّ الإقلاع منها هي فقط.
- بعد أن تقلع منها وتصل إلى سطح المكتب الخاصّ بها، يمكنك تصفّح القرص الصلب على الجهاز ورؤية ما حصل به، ثمّ نسخ ما تريده من ملفّات إلى مكانٍ آمن.
- انتبه، فقد يكون المُخترِق قد وضع فيروساتٍ داخل الملفّات هذه نفسها، وبالتالي لا تتعامل معها على أنّها آمنة (لا تشغّلها حاليًا). قم فقط بنسخها أو رفعها إلى مكانٍ آخر يمكنك الرجوع إليه لاحقًا. ولهذا نستحسن بشدة استخدام نظام لينكس لهذه العملية بدلًا من ويندوز.
- لا تنسخ أيّ برامج؛ انسخ فقط المستندات والصور والملفّات الشخصية، أمّا البرامج وما شابه فلا تنسخها.
- صارت ملفّاتك المهمّة في مكانٍ آخر الآن، لكن لا ضمان لديك أنّها لا تحوي برمجياتٍ خبيثة. عليك تحميلها بصورة مضغوطة (Compressed) ثمّ فك الضغط عنها واستخدام برنامج

مكافحة فيروسات (Anti-Virus) لفحصها. ننصح إمّا بتسليم العملية لشخصٍ متخصص في الموضوع أو استخدام أكثر من مضاد فيروسات للتأكّد من خلو الملفّات من الفيروسات. ننصح كذلك بتصفّحها الواحد تلو الآخر ضمن نظام لينكس (فالفيروسات لا تعمل عليه) وحذف أي ملف مشبوه لم تكن تراه ضمن قائمة ملفّاتك قبل الاختراق.

- يمكنك الآن استعادة هذه الملفّات إلى نظام تشغيلك الجديد.
- اقرأ قسم «اختراق الخدمات» لمعرفة الإجراءات الأخرى المتعلّقة بها.

14. 4. ما تفعله عند اختراق الهاتف المحمول

للأسف لا يوجد الكثير لتفعله عند اختراق الهاتف المحمول.

مشكلة الهاتف المحمول أنّه مقفلٌ في الكثير من الأحيان من طرف الشركة المصنّعة (Vendor Lock-in) ولهذا فإنّ تغيير نظام التشغيل مثلًا غير ممكن (وإلا سيسبب خسارة الضمان من الشركة) وقد لا يكون ممكنًا تقنيًا أصلًا (Locked Bootloader)، كما لا يمكنك التحكم به بنفس السهولة التي يمكنك التحكم بها بالحاسوب مثلًا. إن كان الجهاز ما يزال تحت الضمان فننصح حينها بالاتصال بالشركة صاحبة الضمان فورًا.

الشيء الوحيد لتفعله من طرفك هو إزالة بطاقة الاتصال (SIM) منه، وتعطيل كل الاتصالات (تفعيل وضع الطائرة)، ثمّ وصله عبر منفذ USB إلى حاسوبٍ يعمل بنظام لينكس (إيّاك ثمّ إيّاك وصله بنظام يعمل بويندوز!) لتتمكن من نسخ ملفّاتك المهمة منه. بعدها يمكنك إعادته إلى «وضعية المصنع» (Factory Reset) من الإعدادات مما سيسبب حذف جميع التطبيقات والملفّات والإعدادات عليه.

ستحتاج كذلك إلى استخدام حاسوبٍ لتهيئة بطاقة الذاكرة (SD Card) بالكامل وحذف كلّ شيءٍ منها، وبالتالي ستحتاج إلى قارئ ذواكر (SD Cards Reader) لتشتريه إن لم يكن عندك بالفعل.

لكن لاحظ أنّه حتى ضبط الجهاز إلى وضعية المصنع قد لا يعني التخلّص من الفيروس؛ فقد أصاب مثلًا فيروس xHelper أكثر من 45 ألف جهاز أندرويد سنة 2019م [2] ولم ينفع معه هذا الإجراء، حيث بقي الفيروس ينسخ نفسه من جديد حتّى مع إعادة الضبط إلى وضعية المصنع. وفي مثل هذه الحالات لا بديل من اللجوء إلى المتخصصين.

ستحتاج تثبيت عددٍ من البرامج المُضادة للفيروسات مباشرةً بعد قيامك بضبط الجهاز إلى

وضعية المصنع، ويمكنك البحث عنها من متجر التطبيقات وتثبيتها (ابحث عن كلمة «Antivirus»). بعدها يمكنك استرجاع ملفّاتك تدريجيًا إلى الجهاز (ولا ننصح بذلك ما لم تستشر متخصصًا).

ستحتاج بعدها تأمين الخدمات والحسابات التي كنتَ تستعملها على هذا الهاتف المحمول، وقد شرحنا ذلك في القسم التالي.

قد تضطر عمليًا إلى رمي الهاتف المحمول بالكامل إن لم تستطع التأكّد من خلوه من البرمجيات الخبيثة وشراء واحدٍ جديد كلّيًا.

14. 5. ماذا تفعل عندما يخترقون أحد حساباتك أو خدماتك؟

تختلف الإجراءات التي عليك تنفيذها إذا اكتشفت أنّ بعضًا من حساباتك أو الخدمات التي تستعملها مخترقة بناءً على نوعية الخدمة أو الحساب. فمثلًا إذا اختُرق حساب بريدك الإلكتروني مثلًا فحينها من المتوقّع كذلك أنّ المُختَرِق قد وصل إلى العديد من حساباتك الأخرى كمواقع التواصل أو المعلومات البنكية وغيرها (وهذا لأنّه يمكنه طلب استعادة كلمة المرور وتعيين كلمة مرور جديدة عبر رابط يصل إلى بريدك الإلكتروني، وبما أنّه تحت سيطر المخترق فحينها يمكنه فتح كلّ الحسابات المربوطة بنفس البريد الإلكتروني ثمّ حذف تلك الرسائل الإلكترونية التي تنبّهك عن الموضوع لئلّا تشعر بشيء).

لكن الأهم من ذلك هو أن تعرف كيف تمّت عملية الاختراق؟ هل تمّت عبر برنامج خبيث حمّلته أنت من أحد المصادر المشبوهة ولم تفحصه قبل أن تثبّته، أم هل تمّت عبر هجمات التصيّد الاحتيالي (Phishing Attacks) لهذا الحساب فقط دونًا عن الجهاز كلّه وبقية الخدمات، أم كيف؟ وهذا مهم لأنّه إذا كانت عملية الاختراق قد تمّت عبر تثبيت برنامجٍ خارجي على أحد أجهزتك فحينها لن ينفعك تغيير كلمة المرور للخدمة المُخترَقة وحدها فقط، لأنّ هذا يعني أنّ المُختَرِق يمتلك وصولًا لكل خدماتك وبياناتك وملفّاتك الأخرى.

يمكنك الشروع في إعادة تأمين نفسك عبر الإرشادات التالية بعد أن تكتشف كيف حصلت عمليّة الاختراق - عبر الإرشادات الموجودة في الأقسام السابق - أو عبر استشارة متخصص في المجال.

- إذا اختُرق كامل الجهاز (سواءً هاتف محمول أو حاسوب): غيّر جميع كلمات المرور لكل مواقع وخدمات الويب التي كنت تستعملها عليه بلا استثناء، وكلّ التطبيقات التي تتطلب أيّ نوعٍ من الحماية على الجهاز. وإن كنت تستخدم برنامج إدارة كلمات مرور

(Password Manager) فقم بتغيير كلمة المرور الرئيسة (Master Password) كذلك. هذا بالطبع بعد أن تتبع إرشادات تأمين الأجهزة المخترقة السابق ذكرها.

- إذا اختُرق البريد الإلكتروني: اتصل بقسم الدعم الفنّي لمزوّد خدمة البريد الإلكتروني وأبلغهم بما حصل، وغيّر كلمة المرور الخاصّة به كما غيّر جميع كلمات المرور للحسابات الأخرى التي ربطتها بعنوان البريد الإلكتروني ذاك، كما تأكّد منها وأنّها غير مُخترقة هي الأخرى. وفعّل الاستيثاق الثنائي (2 Factor Authentication) إن كان متوفّرًا.
- إذا اختُرقت خدمة واحدة فقط: كأنّ يُخترق حسابك على فيس بوك فقط دونًا عن بقية حساباتك أو أجهزتك أو أي شيء آخر، فغيّر كلمة المرور للحساب المتعلّق بالخدمة المخترقة فقط (باستثناء ما إذا كنت تستعمل نفس كلمة المرور على مواقع أخرى - وهو ما لا ننصح به بالطبع بل نحذّر منه بشدّة - فحينها غيّر كلمة المرور هناك أيضًا). كما سيكون من المناسب أن تتصل بالدعم الفنّي وتبلغهم مباشرةً عن الحادثة ليخبروك كيف وصل المُختَرق إلى الحساب وماذا فعل به. افحص كذلك النشاطات التي قام بها المخترق عبر حسابك ومالذي فعله به وانظر هل هناك شيءٌ آخر لتراسل الدعم الفنّي حوله أم لا.
- إذا اختُرقت حساباتك وتطبيقاتك البنكية: عليك الاتصال بالدعم الفنّي مباشرةً ثمّ تغيير كلمة المرور وتعطيل بطاقاتك الائتمانية وتغييرها، كما قد يكون المخترق قد قام ببعض عمليات الشراء عبر حساباتك البنكية فعليك حينها إبطالها عبر التواصل مع البنك. لا تكتفي كذلك بالتواصل مع البنك حول الموضوع بل اتصل بالشرطة وأبلغهم عن ذلك وهذا لإخلاء مسؤوليتك من أيّ نشاطاتٍ مشبوهة خارج القانون قد يقوم المخترق بها عبر بياناتك البنكية.

14.6. خاتمة الفصل

اختراق الأجهزة عملية موجعة ومؤلمة جدًا كما ترى والتعامل معها قد يأخذ أيامًا وأسابيع، كما أنّ ضررها قد يبلغ حياة الفرد وماله وسمعته وخصوصيته، بل قد يُقضى على الأجهزة المُخترقة بالكامل إن لم يوجد حلٌ للتخلص من توابع ذاك الاختراق.

ومن أجل هذا جاء المثل الشهير: «درهم وقاية خيرٌ من قنطار علاج»، ومن أجل هذا كتبنا هذا الكتاب، ليكون وقايةً من الوصول إلى هذه الحال بدلًا من التعامل مع تبعات العلاج المستحيلة.

15. مواضيع متقدمة في الأمان الرقمي

أنهينا إلى هنا كلّ المواضيع الأساسية المتعلّقة بحماية المستخدم وأجهزته وخدماته التي يستعملها، كما شرحنا أساسيات الأمان الرقمي والوعي فيه بالإضافة لمواضيع شتّى. وسنتطرق في هذا الفصل الأخير إلى مجموعةٍ من المواضيع المتقدمة المتعلّقة بالمجال.

لا ترتبط هذه المواضيع ببعضها البعض بصورة كاملة لكن من المفيد جدًا أن يطّلع عليها المستخدم ويتعلّمها لزيادة أمانه الرقمي والتعمّق فيه أكثر.

15. 1. الهندسة الاجتماعية

الهندسة الاجتماعية (Social Engineering) هي تصنيف لمجموعة من الممارسات التي يمارسها المخترقون على الضحايا بهدف جعلهم يُضعفون حمايتهم جزئيًا أو كلّيًا طواعيةً بدلًا من الاعتماد بالكامل على اختراق الأنظمة الإلكترونية. قد تشتمل الهندسة الاجتماعية على عمليات اختراق للأنظمة والأجهزة كالمعتاد لكن يجب أن يكون ضمن العملية عامل بشري اجتماعي وإلّا لا يُعتبر ضمن الهندسة الاجتماعية.

رسائل التصيّد الاحتيالي (Phishing) ورسائل البريد والصفحات الإلكترونية المزوّرة كلّها أمثلة على أساليب الهندسة الاجتماعية. فهذه الأساليب مثلًا لا تعتمد على أن يقوم المُختَرِق باختراق جهاز الضحية وسحب البيانات منها بنفسه بسبب ثغرة في البرمجيات مثلًا، بل تعتمد على عوامل نفسية واجتماعية للضحية ليقوم هو بتسليم بياناته الحسّاسة (اسم المستخدم وكلمات المرور مثلًا) للمُختَرق دون أن يعلم بذلك (أو حتّى مع علمه في بعضه الأحيان).

تشمل الأمثلة التي يتّبعها المُخترِقون:

- إرسال صفحة فيس بوك مزوّرة إلى المستخدمين المُراد اختراقهم، وتُسرق حساباتهم عند إدخالهم اسم المستخدم وكلمة المرور.
- إرسال رسائل بريدية أو SMS إلى الضحية المطلوب اختراقها من نوعية: «لقد ربحت مبلغ كذا، أرسل لنا حوالة بنكية صغيرة لنعالج طلب تحويل أموالك» أو «والدك أصيب في حادث سيّارة ويحتاج مبلغًا ماليًا كبيرًا لمتابعة العلاج، أرسل لنا على هذا الحساب البنكي» وما شابه ذلك من اللعب على العواطف.
- اختراق حسابٍ واحد فقط لأحد الموظّفين في أحد المؤسسات التي يريدون اختراقها، ثمّ يستعملون حساباته الإلكترونية لإرسال مستندات ووثائق تحتوي برمجياتٍ خبيثة إلى الموظّفين العاملين مع ذاك الموظّف وهؤلاء بدورهم لن يشكّوا بشيء وسيفتحون الملفّات الخبيثة مباشرةً ويعتبرونها آمنة 100% لأنّها قادمة من صديقهم. ويمكنهم فعل أكثر من ذلك من طلب البيانات الحساسة أو كلمات المرور وسيسلّمونها مباشرةً لأنّ هذا الطلب - يظنّون - قادم من صديقهم أو رئيسهم في العمل، وهكذا تنتشر البرمجيات الخبيثة في كامل المؤسسة وتُسرق جميع البيانات.
- طلبات المساعدة الاجتماعية، مثل «امرأة أرملة ولها طفلان وبحاجة لمساعدة» وما شابه ذلك.

قد تتضمن الهجمات الرقمية مزيجًا من الهجمات على الأنظمة بالإضافة إلى بعض عوامل الهندسة الاجتماعية؛ فيُمكن مثلًا الاعتماد على أحد الثغرات الموجودة في أحد مواقع الويب بالإضافة إلى قيام الضحية بتفعيل إجراء معيّن من طرفه لكي تنجح عملية الاختراق ككل.

من أشهر الأمثلة الحديثة على الهندسة الاجتماعية ما حصل في شركة تويتر مؤخّرًا (شهر يوليو من سنة 2020م) [1]، حيث نجح مراهق أمريكي في الـ17 من عمره بشنّ هجوم هندسة اجتماعية على موظّفي الدعم الفنّي في تويتر ليتمكّن من استخدام بيانات بعضهم للوصول إلى 45 حساب لأشخاص مهمّين حول العالم مثل بيل غيتس ودونالد ترامب وإيلون ماسك وغيرهم، ثمّ نشر عليها تغريداتٍ مزيّفة تدّعي أنّه سيُرسل عملات رقمية (بتكوين) لكلّ من يرسل له مبلغًا بسيطًا على عنوانٍ معيّن. أُلقي القبض على المُراهق وتبيّن أنّه قد جمع أكثر من 100 ألف دولار أمريكي بهذه الطريقة.

المشكلة مع الهندسة الاجتماعية هي أنّها ليست شيئًا يُمكن تأمينه أو الحماية ضدّه؛ فهي في الواقع منبثقة عن مفاهيم الوعي التي شرحناها في أوّل فصلٍ من الكتاب لكنّها قد تستعمل أساليب

متقدمة جدًا لخداع المستخدمين، كما قد تُوظَّف لجلب بيانات هامشية غير مهمّة عن الأنظمة في نظر الناس لكنّها مفيدة جدًا للمُخترقين، حيث يمكن عبر دمجها في عمليات الاختراق الحقيقية للأنظمة أن تصبح مزيجًا مدمّرًا جدًا.

كما أنّه من المستحيل الحماية ضدّها على نطاقٍ واسع؛ فالشركات التي توظّف مئات وآلاف الموظّفين حول العالم وفي مختلف الأمكنة والقطاعات لا تمتلك الموارد الكافية لتحصين كامل موظّفيها وتعليمهم حول هذه المواضيع. وبالتالي فإنّ معظم الأنظمة التي تراها حولك هي قابلة للاختراق في الواقع سواءً من الناحية التقنية أو من الناحية الاجتماعية، لكن ما يردع المخترقين عن محاولة فعل ذلك ليس صعوبة الاختراق بل قدرة الجهات القانونية ومراكز الاستخبارات نفسها على تتبعهم وكشفهم والقبض عليهم كذلك إن فعلوا مثل هذه الأمور، فسلاح الردع هنا ليس الحماية بل هو القدرة على الانتقام من طرف السلطات في حال حصل ذلك.

والهندسة الاجتماعية علمٌ يستعمل في أكثر من مجرّد مجال الأمان الرقمي، بل قد تستعمله الدول بين بعضها البعض لاستمالة الأفراد العاملين في الجهة الأخرى إلى جانبهم وبالتالي اختراقها. وواقعنا الشرق أوسطي خيرُ مثالٍ على ذلك حيث أصبح العملاء والمُخترقون أكثر عددًا من السكّان الأصليين.

يمكنك أنت - كشخص - تحصين نفسك ضد الهندسة الاجتماعية عبر اتباع نصائح الوعي الرقمي التي ذكرناها في مقدّمة هذا الكتاب، ثمّ متابعة قراءة المزيد من الكتب والموارد حولها على الشبكة.

15. 2. الحماية من ثغرات العتاد

يمكن للعتاد كذلك أن يُصاب بالثغرات الأمنية.

إنّ قطع العتاد الموجودة على جهازك - مثل المعالج واللوحة الأمّ - تعتمد على عدّة أشياء لتعمل:

- طرف نظام التشغيل والتعريفات موجودة فيه لقطع العتاد.
- طرف برامج التعريف الثابتة (Firmware) للعتاد نفسه لكنّها لا تخزّن على نظام التشغيل أو القرص الصلب، بل في ذاكرة ROM (وليس RAM) على اللوحة الأمّ.
- طرف العتاد الفيزيائي وطريقة تصميم الدارات الإلكترونية فيه، فهذه الدارات في النهاية تستقبل وتعالج بيانات وبالتالي يمكن لعملياتها هذه أن تكون آمنة أو لا.

أشهر ثغرات العتاد في عصرنا الحالي هما ثغرتا Spectre وMeltdown؛ وهما ثغرتان في أنظمة حماية الذاكرة العشوائية (RAM) أثناء عملها مع معظم المعالجات الحديثة [2]. وقد أصيبت بها جميع معالجات Intel وAMD وARM تقريبًا وترقيعها تطلّب تحديثاتٍ أمنية على المستويات الثلاثة؛ تحديث لتعريفات نظام التشغيل وتحديث لبرامج التحديث الثابتة بالإضافة إلى تعديلات فيزيائية للمعالجات الجديدة لتجنّب هذه الثغرات. وقد كان هذا مكلفًا جدًا على الشركات وكبّدها خسائر كبيرة بالمليارات، كما سببت ترقيعات هذه الثغرات انخفاضًا بأداء الحواسيب يصل إلى 30%.

وهاتان الثغرتان ليستا الوحيدتين بل هناك العشرات من ثغرات العتاد التي اكتُشفت من وقتها. ولهذا على المستخدم متابعة التطوّرات دومًا وتحديث أنظمته وأجهزته إلى آخر الإصدارات.

وتأمين أجهزة المستخدم ضدّها (بعد اكتشافها وإصلاحها من طرف الشركات بالطبع) ممكن عبر تحديث نظام التشغيل أوّلًا بأوّل، ثمّ تحديث برامج التعريف الثابتة (Firmware) وفق إرشادات الاستخدام الصادرة عن الشركات المصنّعة. وفي بعض الحالات يستحيل ترقيع المعالجات القديمة لتجنّب الثغرات وبالتالي يكون من الواجب هنا استبدال كامل الجهاز أو المعالج فيه بواحدٍ أحدث.

15. 3. البيانات الوصفية للملفات وخطورتها

عند مشاركتك لملفٍّ ما مع أحدهم عبر الإنترنت من جهازك فإنّ الملفّ يأخذ معه شيئًا من البيانات الوصفية (Metadata) الخاصّة بك. وهذه البيانات مخفية داخل الملفّ ولا تظهر في محرر النصوص أو البرامج بل تحتاج برامج خاصّة لعرضها. ويختلف حجم وكمّ ونوعيّة هذه البيانات بناءً على نظام التشغيل والبرامج المُستعملة في إنشاء وتعديل الملفّات.

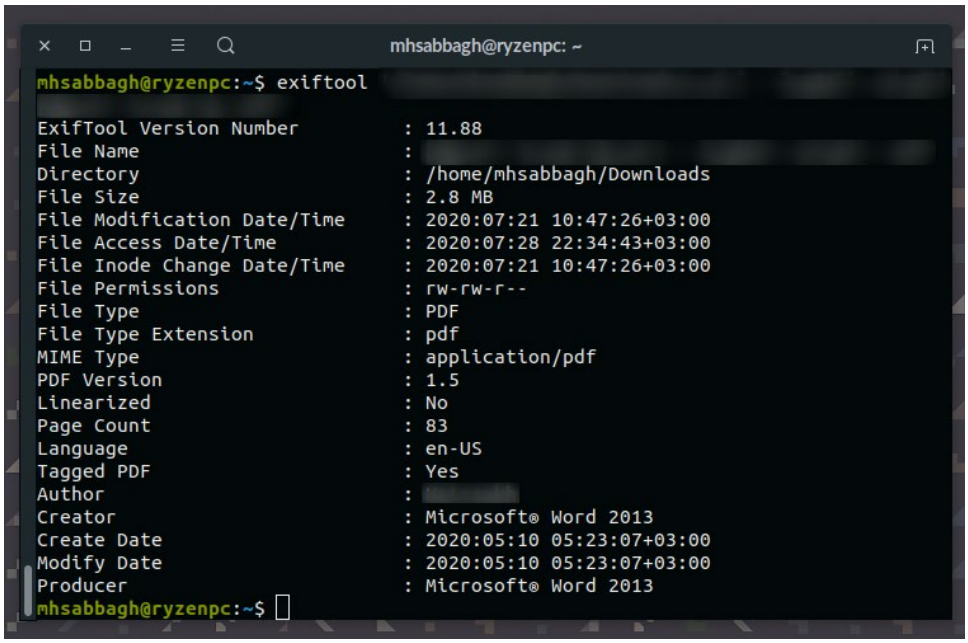
من الأمثلة على البيانات الوصفية:

- تاريخ إنشاء الملفّ لأوّل مرّة.
- تاريخ آخر تعديل على الملفّ.
- تواريخ تعديل الملفّ على فترات مختلفة.
- اسم صانع الملفّ الأصلي.
- اسم من قام بتعديل الملفّ.
- وقت الحرير الإجمالي للملفّ (كم دقيقة قام الناس بالعمل عليه؟).
- اسم البرنامج المُستعمل في إنشاء الملفّ.
- إصدار البرنامج المُستعمل في إنشاء الملفّ.

- وغير ذلك (تختلف البيانات الوصفية بناءً على صيغة الملفّ والبرامج والأنظمة المُستعملة في العمل عليه).

وكما ترى فيمكن لهذه البيانات أن تكشف الكثير عنّ أصحابها وقد تكون معلوماتٍ حسّاسة في بعض الأحيان، وبالتالي - إن كان نموذج الخطر الخاصّ بك مرتفعًا - فعليك إزالتها قبل مشاركتها مع الآخرين. بعضهم يخزّن بيانات الملفّ كاملة في البيانات الوصفية للملفّات ويترك محتوى الملفّ نفسه فارغًا تجنّبًا لإثارة الشبهات في تخزينها داخل الملفّ وهذا ممكن نظريًا :)

يمكنك استعمال برنامج exiftool من سطر الأوامر على لينكس لاستعراض وتعديل وحذف البيانات الوصفية للملفّات. فقط اكتب اسم البرنامج متبوعًا بفراغٍ وبعده مسار الملفّ لرؤية البيانات الوصفية:



يمكنك مراجعة توثيق البرنامج لرؤية طريقة استعماله لتعديل وحذف البيانات الوصفية.

يعمل البرنامج كذلك على أنظمة ويندوز وماك (واجهة نصّية) وبالتالي يمكنك تحميله من موقعه الرسمي على https://exiftool.org

15. 4. نظام Qubes OS وفائدة استخدامه

هناك توزيعات لينكس مختلفة بأنماطٍ متعددة من الحماية لكنّ أبرزها ما يُعرف بـQubes OS، وهي توزيعة لينكس مبنية بنظام الحوسبة الافتراضية (Virtualization) والحاويات (Containers) وهو ما يجعلها من أأمن أنظمة التشغيل في العالم.

طريقة عمل هذه التوزيعة مختلفة عن كلّ توزيعات لينكس الأخرى، فكلّ مكوّناتها من النواة ومكوّنات نظام التشغيل والبرامج الأخرى مفصولةً عن بعضها البعض في حاويات وهمية منفصلة، وبالتالي حتّى لو نجح المخترقون مثلًا في اختراق متصفّح فيرفكس الخاصّ بك فلن يتمكّنوا من الوصول إلى أيّ شيءٍ آخر مخزّن على نظامك ولا حتّى ملفّاتك الأخرى، وهذا لأنّها مفصولة عن حاوية برنامج فيرفكس، وقِس على ذلك.

الحاويات (Containers) هي أشبه بمناطق معزولة في نظام التشغيل تمتلك مواردها وعملياتها الخاصّة بعيدًا عن بقية العمليات الأخرى في نظام التشغيل. مثلًا يمكنك تشغيل توزيعة لينكس (أوبونتو مثلًا) ضمن حاوية على نظام تشغيلك الحالي، وبالتالي تعتبر كأنّها نظام تشغيل وهمي يعمل بصورة منفصلة عن بقية البرامج على نفس نظامك الحالي (لا يوجد إمكانية للبرامج التي تعمل ضمن تلك الحاوية أن تصل إلى ملفّاتك ونظامك الحقيقي). يمكنك تشغيل عشرات ومئات الحاويات في نفس الوقت إن أردت حسب احتياجاتك.

من المفيد أن يطّلع عليها المستخدمون الراغبون في حمايةٍ أكبر على Qubes-OS.org

15. 5. استخدام DNS مشفر منفصل

لقد شرحنا في السابق فائدة استخدام نظام DNS من جهة ثالثة غير نظام الـDNS القادم من مزوّد خدمة الإنترنت الخاصّة بنا في فصل «تأمين الأشياء الأساسية - تأمين الموجّه»، لكن هناك طبقة إضافية من الحماية لأنظمة DNS وهي التشفير؛ حيث يمكنك أن تشفّر الطلبات بينك وبينك نظام الـDNS نفسه كذلك.

هذه الميّزة موجودة فعليًا في متصفّح فيرفكس باسم DNS-over-HTTPS من إعدادات الشبكة ويمكنك تفعيلها:

لكن ما نتحدّث نحن عنه الآن هو نظام DNS مشفّر منفصل كامل تتحكّم أنت به (Dedicated Encrypted DNS)، حيث تثبّته على حاسوب Raspberry Pi صغير مثلًا أو على أحد الخوادم التي تمتلكها، ثمّ تستعمل عنوان الآي بي الخاصّ بذاك الخادوم في الموجّه (الراوتر Router) الخاصّ بك بدلًا من استعمال خدمات شركة خارجية.

والعملية صعبة ومعقّدة بعض الشيء وتتطلب عتادًا منفصلًا ولهذا لم نشرحها في الكتاب، لكن يمكنك معرفة المزيد عبر برنامج DNSCrypt وهو مجاني ومفتوح المصدر ويعمل على الأجهزة والخوادم المختلفة: https://www.dnscrypt.org

15. 6. تحليل تدفق الشبكة

تدفّق الشبكة (Network Traffic) هو البيانات التي تُحمّل وُترفع في شبكة الاتصال المرتبطة بالجهاز. فأيّ جهاز (هاتف محمول أو حاسوب) إمّا يُرسل وإمّا يحمّل البيانات من الشبكة، وبالتالي يمكن تحليل هذا التدفّق ورؤيته لمعرفة بعض المعلومات عنه (الجهة التي يذهب إليها بالإضافة إلى معلومات الترويسات «Headers» وغير ذلك).

وهذا مفيدٌ جدًا لأنّك ستصبح قادرًا على معرفة الاتصالات التي تجريها أجهزتك ومع أيّ خوادم (Servers) وتابعة لمن، وبالتالي يمكنك معرفة ما إذا كنتَ مُخترَقًا أم لا أو إن كان هناك بعض التطبيقات التي ترفع أجزاءً يجب ألّا ترفعها من بياناتك مثلًا. لأنّه بما أنّك تراقب كامل تدفّق الشبكة فيمكنك معرفة ورؤية كلّ الاتصالات التي تجريها أجهزتك على تلك الشبكة.

تحليل التدفّق عملية ممكنة على الحواسيب والأجهزة المحمولة، فقط كلّ ما عليك فعله هو تثبيت أحد برامج تحليل الشبكات (Network Analyzer) على نظام التشغيل المناسب لك ثمّ استعماله وفق التوثيق الرسمي له. لم نشرح العملية في هذا الكتاب لأنّها فوق مستوى القارئ الذي وُجّه له هذا الكتاب لكن العملية ليست أكثر من مجرّد تثبيت البرنامج ثمّ اتباع الشرح الرسمي.

من أشهر برامج تحليل الشبكات على الحواسيب المحمولة برنامجٌ اسمه Wireshark، وهو مجاني ومفتوح المصدر. يمكنك تحميله من موقعه الرسمي وتثبيته على أنظمة ويندوز أو ماك أو لينكس. بعدها يمكنك مراجعة التوثيق الرسمي الخاصّ به لتعلّم استخدامه وكيفية مراقبة تدفّق الشبكة اللاسلكية/السلكية التي أنت متصلٌ بها.

أمّا على الهواتف المحمولة فلا يوجد - على حدّ علمنا - برمجيات مفتوحة المصدر بنفس الجودة والكفاءة. لكن يمكنك البحث في متجر التطبيقات الخاصّ بك عن «Network analyzer» وستجد الكثير من التطبيقات التي يمكنك تجريبها ومراجعتها.

بعد تثبيت البرنامج عليك تشغيله لرؤية أسماء المواقع والخدمات التي تتصل بها أجهزتك. عليك:

- تفحّص الجهاز في الحالة العادية وعلى مدة طويلة (أيام مثلًا)، هل يُرسل بياناتٍ بصورة مفاجئة إلى أحد مواقع الإنترنت أو عناوين آي بي لخواديم معيّنة؟
- تفحّص أي تطبيق تشتبه به أنّه قد يُرسل شيئًا من بياناتك إلى عناوين ويب معيّنة. فقط افتح التطبيق المشبوه وتصفّحه لبضعة دقائق ثمّ راقب تدفّق الشبكة وما إذا كانت تظهر عناوين ويب جديدة يتم الاتصال بها.
- محاولة النظر في محتويات حزم البيانات (Packets) التي تُرسل في تدفّق الشبكة. هل يوجد بها أيّ بيانات حساسة لك؟

قد تُرسل التطبيقات المختلفة على نظامك البيانات إلى عناوين الآي بي (مثل 78.45.4.34) أو إلى أسماء نطاقات مسجّل (example.com). يمكنك فتح تلك العناوين في متصفّحك لرؤية ما إن كانت تعمل وراء خواديم ويب أم لا. إن كان الجواب لا فيمكنك معرفة المزيد عن تلك العناوين (مثل موقعها الجغرافي ولمن هي تابعة) عبر خدمات مثل Who.is.

15. 7. الخدمات اللامركزية

البنية التقليدية للاتصالات في شبكة الإنترنت هي بنية Client-Server (برنامج عميل، برنامج خادوم) حيث يتصل البرنامج العميل (المتصفّح غالبًا) بالخادوم ليجلب البيانات منه، يكون عنوان الآي بي الخاصّ بالخادوم ثابتًا لا يتغيّر ويعرفه كلّ المستخدمين ليتمكّنوا من الوصول إليه عبر اسم نطاق معيّن (Domain Name) يكون مربوطًا به.

لكن هناك بنية أخرى للاتصالات وهي بنية النظير للنظير (Peer to Peer) أو تُعرف رمزًا بـ P2P. وهذه البنية مختلفة عن البنية السابقة حيث لا تتطلب وجود خادومٍ مركزي للاتصال بل تتصل أجهزة العملاء (Clients) بين بعضها البعض مباشرةً لتبادل البيانات. لأنّه بما أنّ كلّ جهازٍ من أجهزتنا يمتلك عنوان آي بي ومنافذ (Ports) خاصّة به فيمكن للأجهزة الأخرى حول العالم كذلك أن تتصل به، إن سمح لها المُستخدم بذلك وعطّل الجدار الناري الخاصّ براوتر الشبكة واستخدم البرامج المناسبة.

أشهر مثال على ذلك هو ما يعرف شعبيًا بالتورنت (Torrent) وله ما يُعرف بالباذرين (Seeders) والنظراء (Peers) الذين يحمّلون البيانات المرفوعة من الباذرين.

لكن صارت الخدمات اللامركزية في السنوات الأخيرة أكثر من ذلك بكثير؛ حيث ضجر الكثير من المستخدمين من سياسات الشركات العملاقة مثل فيس بوك ويوتيوب وجوجل وأمازون وغيرها، ووجدوا أنّ أفضل طريقة لإنشاء محتوىً سهل التداول وغير قابل للحجب والمراقبة وفرض السياسات عليه هو عبر جعله يعمل باتصالات النظير للنظير.

نذكر من بينها المشاريع مفتوحة المصدر التالية:

- Mastodon: أنشئ شبكتك الاجتماعية الخاصّة بك على شكل عُقَد (Nodes) يمكن وصلها بالشبكات الاجتماعية للآخرين أو فصلها متى ما أردت. وهو في الواقع بديل لامركزي لخدمة تويتر.
- Diaspora: شبكة اجتماعية لامركزية أشبه بفيس بوك.
- Beaker Browser: متصفّح ويب يعمل بالكامل بتقنية النظير للنظير، وبالتالي تُنشأ صفحات الويب الخاصّة بك أو تحمّلها من الآخرين عبر الشبكة وبروابط مباشرة بينك وبينهم دون الحاجة للمرور بخواديم أحد.
- Sia: خدمة مشاركة ملفّات لامركزية مثل جوجل درايف وغيرها، لكنّ الملفّات تستضاف على أجهزة جميع المستخدمين بصورة آمنة ومشفّرة ومقطّعة.

15. 8. العملات الرقمية

ظهرت سنة 2009م أوّل عملة رقمية ناجحة وهي بتكوين (Bitcoin). وهي عملة لامركزية تعتمد على تقنية النظير للنظير (Peer to Peer) لإجراء المعاملات المالية الرقمية. والبتكوين في الواقع ما هي إلّا مجموعة بيانات وبالتالي قيمتها قادمة من قيمة السوق المحيط بها والذي يتعامل بها وليست من شيءٍ معيّن.

تخزّن جميع معاملات بتكوين من إرسال وتحويل وغير ذلك في قاعدة بيانات عملاقة مشتركة بين جميع المستخدمين اسمها بلوكتشين (Blockchain)، وهي مشفّرة ومؤمّنة بصورة كبيرة تضمن أنّ المعاملات التي تجري بها غير قابلة للتعديل أو التغيير من قبل الآخرين، وبالتالي يمكن لشخصين مثلًا أن يتبادلا البتكوين بينهما دون خوفٍ من طرفٍ قد يتدخّل بينهما.

إنّ إجراء عمليات بيع وشراء العملات الرقمية يحصل إمّا من طرف محفظات المستخدمين (Users Wallets) مباشرةً بين بعضهم البعض، أو بين منصّات تداول العملات الرقمية (e-Wallets) وهذا هو الخيار الأشهر والأسهل لأنّ الأوّل سيتطلّب الكثير من الجهد والتعب لتأمين البيانات

وإجـراء المعامـلات، بينمـا يمكنـك فـي دقائـق إجـراء عمليـات البيـع والشـراء عـن طريـق أحـد منصّـات العملات الرقمية.

وبفضـل طبيعـة العمـلات الرقميـة فـإنّ تبادلهـا مجهـول تمامًـا، حيـث تحصـل عمليـات تحويـل بتكوين بيـن الأطـراف المختلفـة عـن طريـق عناويـن مشـفّرة مجهولـة الهويـة لا يُعـرف أصحابهـا وبالتالـي تتخفّـى عـن أعيـن المراقبـة (إلّا أنّ الـدول مثـلًا يمكنهـا محاولـة معرفـة صاحـب عنـوان معيّـن عـن طريـق سـجّلات المسـتخدمين وبياناتهـم فـي منصّـات التـداول إن كانـت تحـت أراضيهـا لكـن هـذا غيـر مضمـون).

هنـاك منصّـات عالميـة للتـداول ومنصّـات محلّيـة، ويمكنـك البحـث فـي بلـدك عـن تلـك المنصّـات ورؤيـة مـا إذا كانـت تدعـم البيـع والشـراء داخـل بلـدك أم لا.

هنـاك الكثيـر مـن العمـلات الرقميـة (المئـات وربّمـا الآلاف منهـا) وهـي تجـارة رائجـة جـدًا فـي يومنـا هـذا بـل هـي الموضـة الحاليـة الماليـة فـي عصرنـا. وبسـبب هـذا فقـد ازداد الإقبـال عليهـا فـي العالـم العربـي، لكـن هنـاك العديـد مـن النصائـح والمعلومـات الواجـب تذكّرهـا عنـد التعامـل بالعمـلات الرقميـة:

- لا يمكن استرجاع البتكوين في حال إرسالها إلى عنوانٍ خاطئ أو غير صحيح بتاتًا.
- إن اختُرق حسابك وسُرقت البتكوين منه فقد ضاعت للأبد.
- تحتـاج حاليًـا عمليـات بتكويـن مـا بيـن 10 دقائـق إلـى عدّة سـاعات لإجراء مـا يعـرف بالتأكيدات (Confirmations) وهـي ببسـاطة عمليـات التأكّـد مـن نظيريـن (Peers) آخريـن مـن العمليـة وأنّها صحيحة.
- إنّ إنشـاء محفظتـك الخاصّـة بـك للعمـلات الرقميـة علـى حاسـوبك هـو الخيـار المنصـوح بـه لكنّـه مـن المسـتحيل علـى معظـم قـرّاء هـذا الكتـاب تطبيقـه لصعوبتـه وصعوبـة تأميـن الأمـوال التـي عليـه بعدهـا، وبالتالـي فـإنّ أفضـل حـلّ هـو اسـتخدام المنصّـات الجاهـزة للعمـلات الرقميـة.
- هناك رسوم استقبال وإرسال تؤخذ منك من قبل تلك المنصّات عند كلّ عملية تجريها.
- منصّـات التـداول خاضعـة للـدول التـي تعمـل بهـا وبالتالـي هـي تحـت قوانينهـا، وهـي تمتلـك كامـل معاملاتـك الماليـة معهـا بالإضافـة إلـى كلّ عناويـن الاسـتقبال التـي اسـتعملتها وبالتالـي يمكنهـا معرفـة نشـاطاتك بالتعـاون مـع الدولـة. وتسـتعمل الـدول تلـك المعلومـات غالبًـا مـن أجـل جمـع الضرائـب كمـا فـي حالـة Coinbase والولايـات المتّحـدة.
- اسـتعمل نصائـح تأميـن الحسـابات التـي شـرحناها مسـبقًا فـي هـذا الكتـاب لتأميـن حسـابك علـى تلـك المنصّـات، مثـل اسـتخدام الاسـتيثاق الثنائـي وكلمـة مـرور قويـة وغيـر ذلـك.

15. 9. متابعة آخر أخبار الحماية والأمان والخصوصية

يمكنك متابعة آخر أخبار الحماية والخصوصية بالإضافة إلى آخر التطورات والأبحاث في المجال عن طريق متابعة المواقع والمراكز التالية. وتمامًا كما هناك ما يسمّى بـ«مراكز التفكير» (Think Tanks) في السياسة فهناك مراكز أبحاث شبيهة في الأمان الرقمي.

- CitizenLab: مركز أبحاث حول الأمان الرقمي مركزه في كندا، لديه العشرات من التقارير والأبحاث المهمّة حول الخصوصية والأمان في العصر الحديث لم يُسبَق إليها من قبل.
- Upturn: مركز أبحاث أمريكي متخصص بانتهاكات الخصوصية وسبل الوقاية منها وأساليب كسرها.
- The Hacker News: موقع إخباري متخصص في أخبار الاختراقات والحماية حول العالم.
- r/Privacy: على موقع ريديت: مجتمع متخصص بالخصوصية وآخر أخبارها على منصة النقاش الشهيرة Reddit.
- Information Security StackExchange: ليس موقعًا لمتابعة آخر الأخبار بل منصة أسئلة وأجوبة حول الأمان الرقمي. يمكنك الاستفادة من قراءة الأسئلة هناك أو طرح أي سؤال تريده عن مجال الأمان الرقمي.

ينتهي هنا «دليل الأمان الرقمي» بعد أكثر من 15 فصلًا مختلفًا عن تأمين المستخدم لأجهزته وخدماته ومعاملاته للحفاظ على أمانه وخصوصيته الرقميين.

إنّ الأمان الرقمي لم يعد شيئًا رفاهيًا يُمكن غضّ النظر عنه أو التقليل من قيمته، ولا هو شيءٌ بسيط لا يحتاج تفكيرًا ولا جهدًا لإعداده، بل كما بيّنا قد يستغرق الكثير من الوقت والجهد إلّا أن النتيجة طيّبة بإذن الله؛ من حفظ الإنسان وقته وماله وبياناته وتعب عمره من الضياع أو الاختراق.

نذكّر مرّةً أخرى هنا أنّ هذا الكتاب كان يستهدف الجمهور العريض من المهتمين العرب بمجال الأمان الرقمي وأننا غطّينا معظم المواضيع الأساسية والمهمّة للفئة الأكبر من المستخدمين، لكن ما يزال هناك الكثير من المواضيع الأخرى في المجال والتي يمكنك أن تتوسع فيها بمفردك، أو لعل المهتمين بالمجال يبحثون عن مصادر أخرى للتعمّق فيه، وليس هذا الكتاب شاملًا لكلّ المواضيع في الأمان الرقمي بحالٍ من الأحوال، إلّا أننا غطّينا ما أمكن تغطيته.

إنّ الموارد العربية عن مجال الأمان والخصوصية في العالم العربي شحيحةٌ للأسف؛ وترجع

الأسباب كثيرًا إلى بُخل الخبراء في نشر المعلومة بالإضافة إلى احتكارها والتفكير فيها بصورة ماديّة بحتة فقط، غير مُبالين بما يخلّفونه وراءهم من مستخدمين معرّضين للانتهاك في أيّ لحظة بسبب غياب الكتب والشروحات التعليمية المفيدة في المجال.

ولكنّ الوضع يتحسّن؛ وما هذه المبادرة المدعومة من طرف شركة حسّوب بالإضافة إلى مشاريع المحتوى العربي الكثيرة الأخرى إلّا بداية الغيث إن شاء الله.

سائلين الله القبول وأن يكون عملنا هذا خالصًا لوجهه، وأن تكون كلّ معلومةٍ مذكورةٍ في هذا الكتاب قد أفادت أحدهم وحمته أن يضيع بياناته.

أحدث إصدارات أكاديمية حسوب

حسوب
HSOUB.COM